Principles of Information Operations: A Recommended Addition to U.S. Army Doctrine

A Monograph
by
LTC Gerald V. Burton, Jr.
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas
First Term AY 02-03

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
22-05-2003	monograph	18-06-2002 to 22-05-2003

4. TITLE AND SUBTITLE
Principles of Information Warfare:
A Recommended Addition to U.S. Army Doctrine
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Burton, Jr., Gerald V. ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
US Army School of Advanced Military Studies
Eisenhower Hall
250 Gibbon Ave
Fort Leavenworth, KS66027

8. PERFORMING ORGANIZATION REPORT NUMBER
ATZL-SWV

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT

It is imperative that Army doctrine fulfill its mandate to create common understanding across the force. This includes establishing a common basis for conducting IO across the spectrum of conflict. Army IO doctrine must provide commanders and their staffs the foundation necessary to effectively integrate IO into full spectrum operations. Without successful IO, achieving information superiority is unlikely. Without information superiority, the Army is at risk of failing to accomplish its assigned missions in the decisive manner that is expected and necessary. The soon to be released FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures, represents a leap ahead in Army thinking about IO. It is particularly good at describing the IO threat and how the IO elements and related activities interact. It also presents numerous and detailed tactics, techniques and procedures for conducting (planning, preparing, executing and assessing IO). Still, this monograph asserts that FM 3-13 lacks a general, macro-level articulation of how IO elements are combined, so it needs to add a set of principles that guide commanders and staffs on how to combine the IO elements. This monograph seeks to discover whether or not existing U.S., Russian, and Chinese doctrine and theory can provide the sought after guidance on combining IO elements. The answer is yes. An analysis of all three nations? writings on IO, and synthesis of the related ideas, shows they do offer potential solutions to the problem. These solutions are offered as recommended improvements to the ongoing Army IO doctrine debate. The monograph subscribes to the idea that IO is an integrating strategy, relating means to ends. Combining the elements is the essential part of this strategy, and must be guided by six principles. First, commanders and staffs must understand and leverage all three domains of IO: physical, cognitive and information. Second, they must use a systems approach to understand the environment. Third, commanders and staffs must use an effects based approach for relating means to ends and for recognizing the outcomes of actions, both desirable and undesirable. Fourth, they must use analogues to develop targets. Fifth, commanders and staffs must arrange IO activities in time, space and purpose to mass effects. Sixth, they must leverage ISR to support planning, preparing, executing and assessing IO. In making the case for these principles, the monograph covers several key areas. It discusses the IO environment in relation to the problem. It explains the three domains, provides a basic understanding of open systems, and shows how applying an effects-based methodology to IO can benefit the Army. Several models are also proposed to assist in target selection and arranging IO activities in time, space and purpose. Overall, the monograph offers concrete recommendations for how to think about combining the IO elements (and related activities), which is the heart of IO as an integrating strategy. Adopting the recommended principles can help the Army conduct IO more effectively. With effective IO, the Army is much more likely to be decisive in all its missions.

15. SUBJECT TERMS
United States; Army; Information operations; FM 3-13; Russian doctrine; Chinese doctrine; Target selection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
			Same as Report (SAR)	70	Buker, Kathy kathy.buker@us.army.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 913758-3138 DSN 585-3138

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

LTC Gerald V. Burton, Jr.

Title of Monograph: Principles of Information Operations: A Recommended Addition to U.S. Army Doctrine

Approved by:

_____ Monograph Director
Timothy L. Thomas, M.A.

_____ Director, School of
COL James K. Greer, MMAS Advanced Military Studies

_____ Director, Graduate Degree
Philip J. Brookes, Ph.D. Program

PREFACE

This monograph grew out of my personal intellectual struggle to figure out how an Information Operations Officer (Functional Area 30) does his or her job. It is a difficult but rewarding field. We have come a long way in five years, and still have far to go. This is my attempt help us continue our journey. I have learned a great deal while writing this monograph, but I have also raised many new questions. I look forward to seeking out the answers.

As I wrote this monograph, we all faced significant challenges and changes. Still, for me it was a time full of professional, personal and spiritual growth. I want to thank my SAMS classmates and the faculty for helping me learn so much this year. I am also grateful to my Monograph Director, Tim Thomas, for his patience and guidance. I also want to express my appreciation to my parents, friends and fellow military professionals whose care and support has benefited me over the years. As far as my family, I cannot say enough about how wonderful they are. My wife and daughters are the light and salt of my life. Their never-ending devotion, sacrifice and love over the last year (and always) allowed me to finish. Thanks! Finally, I give praise to the Lord for all the blessings he has bestowed upon us.

ABSTRACT

PRINCIPLES OF INFORMATION OPERATIONS: A RECOMMENDED ADDITION TO U.S. ARMY DOCTRINE, by LTC Gerald V. Burton, Jr., USA, 50 pages.

It is imperative that Army doctrine fulfill its mandate to create common understanding across the force. This includes establishing a common basis for conducting IO across the spectrum of conflict. Army IO doctrine must provide commanders and their staffs the foundation necessary to effectively integrate IO into full spectrum operations. Without successful IO, achieving information superiority is unlikely. Without information superiority, the Army is at risk of failing to accomplish its assigned missions in the decisive manner that is expected and necessary.

The soon to be released FM 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures*, represents a leap ahead in Army thinking about IO. It is particularly good at describing the IO threat and how the IO elements and related activities interact. It also presents numerous and detailed tactics, techniques and procedures for conducting (planning, preparing, executing and assessing IO). Still, this monograph asserts that FM 3-13 lacks a general, macro-level articulation of how IO elements are combined, so it needs to add a set of principles that guide commanders and staffs on how to combine the IO elements.

This monograph seeks to discover whether or not existing U.S., Russian, and Chinese doctrine and theory can provide the sought after guidance on combining IO elements. The answer is yes. An analysis of all three nations' writings on IO, and synthesis of the related ideas, shows they do offer potential solutions to the problem. These solutions are offered as recommended improvements to the ongoing Army IO doctrine debate.

The monograph subscribes to the idea that IO is an integrating strategy, relating means to ends. Combining the elements is the essential part of this strategy, and must be guided by six principles. First, commanders and staffs must understand and leverage all three domains of IO: physical, cognitive and information. Second, they must use a systems approach to understand the environment. Third, commanders and staffs must use an effects based approach for relating means to ends and for recognizing the outcomes of actions, both desirable and undesirable. Fourth, they must use analogues to develop targets. Fifth, commanders and staffs must arrange IO activities in time, space and purpose to mass effects. Sixth, they must leverage ISR to support planning, preparing, executing and assessing IO.

In making the case for these principles, the monograph covers several key areas. It discusses the IO environment in relation to the problem. It explains the three domains, provides a basic understanding of open systems, and shows how applying an effects-based methodology to IO can benefit the Army. Several models are also proposed to assist in target selection and arranging IO activities in time, space and purpose. Overall, the monograph offers concrete recommendations for how to think about combining the IO elements (and related activities), which is the heart of IO as an integrating strategy. Adopting the recommended principles can help the Army conduct IO more effectively. With effective IO, the Army is much more likely to be decisive in all its missions.

TABLE OF CONTENTS

PREFACE i
ABSTRACT ii
TABLE OF CONTENTS iii
ILLUSTRATIONS v
TABLES vi
CHAPTER ONE: INTRODUCTION 1
CHAPTER TWO: BACKGROUND 4
Problem 4
Foreign Information Operations 9
The Russian Approach to IO 10
The Chinese Approach to IO 12
A Few Words on Terminology 12
Information and Information Systems 12
Information Operations vs. Information Warfare 13
CHAPTER THREE: DISCUSSION 14
Environmental Factors Affecting the Conduct of IO 14
IO Crosses Multiple Domains 14
IO Spans the Entire Depth of the Operational Environment 16
IO Involves a Wealth of Actors 17
IO as an Integrating Strategy 17
The Effects-Based Approach to IO 19
The Systems Approach 22
The Importance and Challenges of ISR in Supporting IO 25
Pros and Cons of an Effects-based Approach 26
IO Targets 27
The Stratagem Approach to IO 32
Arranging the IO Elements in Time, Space and Purpose 35
CHAPTER FOUR: CONCLUSIONS AND RECOMMENDATIONS 38
Determining Assessment Criteria 38
The Utility of Foreign IO 39
Conclusions 39
Domains 39
Systems 40
Effects 41
Targeting Models 42
Time, Space and Purpose 42
ISR 44
Recommendations 45
Final thoughts 48
APPENDIX A: FURTHER DEFINING INFORMATION AND IO 49
Other Definitions of Information 49
Russian Definitions of Information Operations 50
Chinese Definitions of Information Operations 50
APPENDIX B: TYPES OF IO EFFECTS 52
GLOSSARY 55
BIBLIOGRAPHY 57

Books 57
Government Publications 58
Articles 59
Translated Documents 60
Monographs, Reports, Theses, and Unpublished Works 61
Other Internet Sources 62

ILLUSTRATIONS

Figure 1. Graphic Example of Direct and Indirect Effects 20
Figure 2. Information-based Targeting Model 29
Figure 3. Domain-based Targeting Model. 30
Figure 4. Military Function-based Targeting Model. 32
Figure 5. Arranging IO in Time, Space and Purpose 43
Figure 6. IO Effects List. Source: JIWSOC briefing, Class R-00-6, July 2000 53

TABLES

Table 1. Types of Effects……21
Table 2. IO Activities and Effects……...37

CHAPTER ONE

INTRODUCTION

Information operations (IO) emerged as a new and distinct concept following Operation Desert Storm. Since then, many observers and leaders feel IO is of increasing importance, especially as the U.S. prosecutes the war on terrorism and executes other operations as directed by national leaders. The Army is therefore challenged to demonstrate maturity in thought and deed as it conducts IO under wartime conditions.

Experience, history, doctrine and theory are among the traditional guides for the professional soldier in doing his or her duties. Since IO is a new concept, the Army has limited experience and history to draw on when compared to the 228 years of fire, maneuver, leadership and other traditional elements of combat power. Theories purporting to describe IO abound. Dr. James Schneider states "military theory is a professionally justifiable, reliable system of beliefs about the nature of war."[1] Applying this definition, there is no comprehensive theory for IO. So the Army is left to rely on doctrine for helping commanders and their staffs plan, prepare, execute and assess IO.

Given this situation, it is imperative that Army doctrine fulfills its mandate, giving the Army a common basis for conducting IO. Army IO doctrine must include a thorough, intellectual and pragmatic explanation of IO. It must provide commanders and their staffs the foundation necessary to effectively integrate IO into Army full spectrum operations as prescribed in Field Manual (FM) 3-0, *Operations*. Without that, IO is unlikely to be a valuable contributor to information superiority. Without information superiority, the Army is at risk of failing to accomplish its assigned missions in the decisive manner that is expected and necessary.

[1]James J. Schneider, "How War Works: The Origins, Nature and Purpose of Military Theory, 2001," unpublished paper, p. 9, School of Advanced Military Studies, Ft. Leavenworth, KS.

The soon to be released FM 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures*, attempts to meet this mandate. The new FM represents a leap ahead in Army thinking about IO. Still, this monograph asserts that FM 3-13 lacks a general, macro-level articulation of how IO elements are combined, so it needs to add a set of principles that guide commanders and staffs on how to combine the IO elements.

This monograph seeks to discover whether or not existing U.S., Russian, and Chinese doctrine and theory can provide the sought after guidance on combining IO elements. The answer is yes. An analysis of all three nations' writings on IO, and synthesis of the related ideas, will show they do offer potential solutions to the problem. These solutions are offered as recommended improvements to ongoing Army IO doctrine debate.

Summarizing the recommendations, the monograph subscribes to the idea that IO is an integrating strategy, relating means to ends. Combining the elements is the essential part of this strategy, and must be guided by six principles. First, commanders and staffs must understand and leverage all three domains of IO: physical, cognitive and information. Second, they must use a systems approach to understand the environment. Third, commanders and staffs must use an effects based approach for relating means to ends and for recognizing the outcomes of actions, both desirable and undesirable. Fourth, they must use analogues to develop targets. Fifth, commanders and staffs must arrange IO activities to mass effects. Sixth, they must leverage ISR to support planning, preparing, executing and assessing IO.

While the major points of the monograph have been outlined already, a slightly more detailed overview of the methodology is in order. This first chapter is merely a short overview and introduction to the monograph. The second chapter sets the stage for digging into the problem. It defines the problem, and bounds the discussion by describing important terms and ideas related to IO. It also explains why and how foreign IO writings are important to the problem at hand. Chapter Three is a lengthy discussion on developing guidance for effectively combining IO elements. It analyzes relevant ideas regarding the subject, including key environmental factors.

The fourth and final chapter synthesizes the arguments made in the previous chapter to produce conclusions that form the basis of the recommendations.

CHAPTER TWO

BACKGROUND

> *The only thing harder than getting a new idea into the military mind is to get an old one out.*
>
> *-- B.H. Liddell Hart*[2]

This chapter begins with a discussion of the problem with Army IO doctrine as promulgated in FM 3-13, which is due to be released any day. It describes how that doctrine has matured quickly and significantly, but lacks guidance on combining the IO elements. The chapter continues by proposing to use existing doctrine, along with theoretical writings to find ways to rectify this problem. It will propose using Russian and Chinese as well as US writings for this purpose, and explain why. Finally, it will explain some definitions and assumptions being made regarding IO. At the end of this chapter, the foundation will be laid for launching a review and analysis of IO literature.

Problem

A relatively new concept, IO can be used to create synergy in combining formerly separate functions to dominate the information battlespace.[3] The concept has grown fast. The Army's first and only IO unit, 1st Information Operations Command (Land), formerly the Land InformationWarfare Activity, was activated in 1995.[4] The first Army doctrine was published in 1996, and the first joint doctrine followed two years later. The Army created a functional area for IO officers under the Officer Personnel Management System XXI (OPMS XXI) in 1997.[5] While

---

[2]B.H. Liddell Hart, quoted in James Charlton, ed., *The Military Quotation Book* (New York: St. Martin's Press, 1990), 65.

[3]Department of the Army, *FM 3-13 Information Operations Doctrine, Tactics, Techniques and Procedures (Approved FinalDraft)* (Washington, D.C.: GPO, 2002), 1-1.

[4]*Land Information Warfare Activity* (Fort Belvoir, VA: Land Information Warfare Activity, 1998), 1.

[5]LTC Donna L. Coffman, "OPMS to OPMS XXI: Then, Now and the Future - What does it mean to the Quartermaster officer?," Quartermaster Professional Bulletin, Autumn 1997. <http://www.quartermaster.army.mil/oqmg/Professional_Bulletin/1997/Autumn/opmsxxi.html> (March, 13, 2003).

growth has been fairly rapid, experience from the field shows there is a learning curve associated with effectively integrating IO into Army operations.

Lessons learned during the Battle Command Training Program (BCTP) reflect the need for better understanding of IO by Army staffs. The BCTP staff found many divisional staff members do not appreciate what IO adds to the fight. Staffs tend to stay in their comfort zone, rather than deal with the uncertainties of IO. This is especially true if the Chief of Staff or the IO Coordinator is not actively engaged in integrating staff activity towards the fulfillment of IO objectives. There has been a tendency to associate IO primarily with force protection, disregarding the offensive potential of IO. This is a negative lesson picked up in security and stability operations in the Balkans.[6] Overall, these trends tend to reflect a lack of understanding of IO and/or a lack of knowledge on how to conduct it. The Army needs a way to overcome these deficiencies.

One of the ways to overcome such deficiencies is through doctrine. As stated in FM 3-0, the Army's capstone operational publication, "Army doctrine provides a common language and a common understanding of how Army forces conduct operations."[7] In his foreword, the Army Chief of Staff says "FM 3-0, *Operations*, discusses … how to apply combat power, and how to think about operations. In short, it provides a professional intellectual framework for how we operate."[8] Doctrine enhances the Army's ability to communicate and supports a common culture—if it is widely known and understood.[9] Doctrine then, is a vehicle that can help the Army quickly develop IO capabilities sorely needed in the global war on terrorism and other operations.

---

[6]Roy Hollis, "Information Operations Observations, TTP, and Lessons Learned," Center for Army Lessons Learned. November 2001, <http://call.army.mil/products/trngqtr/tq3-02/hollis.htm> (March 3, 2003).

[7]Department of the Army, *FM 3-0 Operations* (Washington, D.C.: GPO 2001), 1-14.

[8]Ibid., inside cover.

[9]Ibid., 1-14.

Army IO doctrine is evolving. The overarching guide for all Army doctrine, including IO, is FM 3-0.[10] Published in June 2001, FM 3-0 describes IO as one of three contributors to information superiority, along with information management (IM) and intelligence, surveillance and reconnaissance (ISR). Information superiority (IS) is a type of enabling operation that supports the four types of Army operations: offensive, defensive, stability and support. In FM 3-0, IO is defined as " actions taken to affect adversary, and influence others', decision making processes, information and information systems while protecting one's own information and information systems." It also lists twelve elements and two related activities of IO, as well as stating the existence of offensive and defensive IO.[11]

The Army's current IO doctrinal manual, FM 100-6, is outdated. When FM 3-0 was published in 2001, it codified a significant change in the Army's views on IO. A replacement for FM 100-6, renumbered FM 3-13, is in approved final draft form. Dated October 2002, FM 3-13 articulates Army IO doctrine in a fashion relatively consistent with FM 3-0.[12] It states: "Commanders conduct (plan, prepare, execute and assess) information operations (IO) to apply the information element of combat power." They "conduct IO by synchronizing the IO elements and related activities, each of which may be used either offensively or defensively."[13] Between FM 3-0 and FM 3-13, the Army is showing consistency, depth and maturity of thought greatly needed in IO. This promises to make FM 3-13 a big improvement over its predecessor.

Field Manual 3-13 is useful in several ways. Chapter 1 lays out the information environment, the threat, and the categories of IO (offensive and defensive). It also describes the object of IO, which is information superiority.[14] Later chapters promulgate operations security and deception

[10]Ibid., vii.
[11]Ibid., 11-1 to 11-24.
[12]The time gap between FM 3-0 and this manual allow for some updated information, such as a slight reorganization of IO elements.
[13]*FM 3-13,* 1-1.
[14]Ibid., 1-1.

doctrine for the Army. In essence, it provides a general, macro-level view of the who, what, when, where and why of IO.

Chapter 2 of FM 3-13 describes "the contributions and links of each IO element and related activity."[15] In this chapter, there are 12 IO elements and 2 related activities. The core elements are Operations Security (OPSEC), Psychological Operations (PSYOP), Military Deception, Electronic Warfare (EW), Computer Network Operations (CNO: with subsets of Computer Network Attack, or CNA, and Computer Network Defense, or CND) and Computer Network Exploitation (CNE). The supporting elements are Physical Destruction, Information Assurance (IA), Physical Security, Counterintelligence (CI), Counterdeception and Counterpropaganda. The related activities are Public Affairs (PA) and Civil-Military Operations (CMO).[16] The manual does not specifically state the difference between core and supporting elements.

Where FM 3-13 falls short is describing *how* to conduct IO. Starting with Chapter 5, the manual proscribes tactics, techniques and procedures (TTP) for IO.[17] By definition, TTP go into details. Tactics describe how units are employed. Techniques give the methods of using equipment and personnel to perform their mission. Procedures are "standard and detailed courses of action that describe how to perform tasks."[18] The TTP provide excellent micro-level guidance for personnel specifically tasked to perform IO-related duties. Yet this approach overlooks the possibility that there may be some general concepts that would help not just the Army IO community, but a broader Army audience as well.

Field Manual 3-13 claims to support commanders and staffs from brigade to Army Service component level.[19] At these levels, there are maneuver commanders, operations officers, fire support personnel, intelligence specialists and a host of others that either integrate or support IO during the course of their duties. They only need to understand the how to conduct IO at a macro-

[15]Ibid., 1-1 to 2-33.
[16]Ibid., 2-1.
[17]Ibid., 5-1.
[18]Department of the Army, *FM 3-90 Tactics (*Washington, D.C.: GPO, 2001) 1-2.

level. That is the value of doctrine: providing a common understanding across the Army.[20] As written, FM 3-13 does not offer a macro-level understanding of how to conduct IO. It only provides a micro-level one. It must address this problem if it is to be useful at all levels.

The way to fix this problem may be implied from FM 3-0. It clearly states that doctrine for full spectrum operations-offense, defense, stability and support operations-depends on certain fundamentals.[21] These fundamentals provide the *conceptual foundations* for field execution and classroom education, as well as the basis for efficient and effective force employment. The Army is decisive in all its efforts through knowledge and application of the fundamentals.[22] If Army operations as a whole are grounded in such fundamentals, then IO probably should be as well.

The principles of war are a constituent part of fundamentals listed in FM 3-0. The principles guide and instruct commanders in combining the elements of combat power: maneuver, firepower, leadership, protection and information.[23] Further, the principles "provide general guidance for conducting war and military operations other than war (MOOTW) at the strategic, operational and tactical levels."[24]

Commanders and their staffs apply the information element of combat power via IO.[25] The IO elements are the components of the information element of combat power.[26] Therefore, it is reasonable to assume that IO should have some general guidance for commanders (and staffs), who have to determine *how* to combine the IO elements, during war and MOOTW and at all levels of war.[27] It becomes clear that this is what FM 3-13 does not address beyond the TTP -- IO needs its own set of principles to explain in general terms the "*how*" of IO.

---

[19]*FM 3-13,* iii.
[20]*FM 3-0,* 1-14.
[21]Ibid., 4-2.
[22]Ibid.
[23]Ibid.
[24]*FM 3-13,* 4-11.
[25]Ibid., 1-1.
[26]Ibid., 1-14.
[27]Department of Defense, *JP 3-13 Joint Doctrine for Information Operations* (Washington, D.C.: GPO, 1998), vii. Additionally, *JP 3-13* says IO apply across the range of military operations, which

This monograph asserts that doctrine lacks a general, macro-level articulation of how IO elements are combined. The monograph seeks to address this problem by recommending a set of principles that guide commanders and their staffs in combining the IO elements in order to meet commanders' objectives. The discussion and conclusions in the following chapters seek to identify what those principles are. The discussion assumes that the answers lie not just in the writings, doctrinal and theoretical, of U.S. IO proponents.

Foreign Information Operations

American military theorists and doctrine writers have borrowed from the works of Sun Tzu, Clausewitz and Svechin for years. In that same vain, U.S. Army IO doctrine writers can learn from Russia and China. They are two of several countries that have offered different approaches to IO. The unique cultural outlook of these two powers, both of whom are pursuing their own IO programs, should add value to the discussion presented here.

This monograph does not attempt to redefine doctrinal views of the IO threat. The final draft of FM 3-13 already elaborates on generic threat capabilities. Instead, this monograph will review Russian and Chinese IO theories for relevance to the problem at hand—guidance on combining IO elements. Russia and China were chosen over other nations for two reasons. First, their body of literature on the subject is large enough for drawing conclusions. Second and more importantly, their opinions represent potentially significant dissimilarities with the U.S. This contrast of ideas could stimulate improvements in U.S. doctrine.

There are obviously vast cultural, experiential, political and other differences between U.S., Russian and Chinese theories of war. Attempts to decipher the meaning and utility of every nuance of Russian or Chinese theorists would be fruitless and potentially counterproductive. Therefore, this monograph will only extract that which relates to the thesis of this monograph, principles for how to combine IO elements.

---

according to *JP 3-0* (I-2) includes war and MOOTW. *FM 3-13* (1-18) says commanders integrate IO at all levels of war.

One other key point for understanding Russian and Chinese writings is that they do not publish doctrine as we do. The writings considered in this monograph are not necessarily approved or official. They may in fact be inconsistent with actual practice, and/or intentionally misleading.[28] Nevertheless, they hold value if they discuss ways to address the identified problem in U.S. doctrine. There are specific peculiarities expected from each body of foreign literature. The following paragraphs address these peculiarities to provide context for the upcoming discussion.

The Russian Approach to IO

Russian thinkers approach IO from a different perspective. The nature of their economic and technological situation, politics, culture and military experience significantly influences their thinking.

Russia's inferior technological state with regards to the West, largely connected to its poor economic conditions, affects their attitudes towards IO. On one hand, they see foreign use of IO as a threat to their politically and culturally vulnerable society. On the other, it offers capabilities they currently only have a limited ability to use.[29]

Russian political and cultural history creates a different basis for thinking than the West. Russian aims, moral laws and Marxist ideology all shape their analysis. Further, the dialectic, or logical view derived through "dialogue and intellectual investigation," is a huge factor in how Russian thinkers look at the problems of IO.[30]

---

[28]Timothy L. Thomas, "The Russian Understanding of Information Operations and Information Warfare," in *Information Age Anthology: The Information Age Military*, ed. David S. Alberts and Daniel S. Rapp, (Washington, D.C.: DOD C4ISR Cooperative Research Program, 2001) 779-780.

[29]Thomas, "The Russian Understanding," 777-779.

[30]Timothy L. Thomas, "Russia's Asymmetrical Approach to Information Warfare," in *The Russian Military into the 21st Century* (London: Frank Cass Publishers 2001), 8-9. Page references are to a copy of the article provided to the author by Mr. Thomas.

The Russian study of military theory is highly structured and thorough, including among other things a clearer distinction between military art and science. Russian open source writings, while limited, tend to focus on theory, vice the trend towards practical aspects in the West.[31]

Three other factors make the Russian approach different from the U.S. one. They can be tied to Russia's current lack of technological competitiveness and traditional concepts of modern military operations and strategy. First, Russians expect to rely more on a large, synergistic application of all available means to disorganize their opponent's information capability.[32] The second difference is Russia's desire to focus on manipulating an opponent's cognitive processes, or what they consider the "information-psychological" aspect of IO. In essence, they seek to affect the enemy's reasoning and decision-making processes to produce outcomes favorable to Russian objectives, without the enemy realizing it. This can include means that might be considered highly unusual in the U.S., such as the use of parapsychology, bioenergy, and acoustics, to name a few.[33] Closely related to the information-psychological aspect is the theory of "reflexive control," a sophisticated Russian version of perception management.[34] Third, unlike the U.S., the Russians define a concept for "information weapons." As means to change the information processes of targeted information systems, they offer tools for conducting IO.[35] Overall, their writings indicate they seem to have thought much more deeply about how to target, affect and assess IO efforts meant to influence the enemy mind than their U.S. counterparts.[36]

---

[31]Thomas, "The Russian Understanding," 778-779.

[32]Thomas, "Russia's Asymmetrical Approach," 11-13.

[33]Timothy L. Thomas, "Human Network Attacks," *Military Review* (September-October 1999): <http://fmso.leavenworth.army.mil/fmsopubs/issues/humannet/humannet.htm> (August 30, 2002).

[34]Ibid.

[35]Ibid.

[36]Thomas, "Russia's Asymmetrical Approach," 11-14.

The Chinese Approach to IO

Like the Russians, Chinese writers approach IO from a unique slant. Their view of their own history is one of a nation perennially at war, often abused by outside powers.[37] Therefore it is not surprising they see themselves as the perennial underdog, always inferior militarily to the threats they face. This perception serves as a basis for the next two features of the Chinese approach. The influence of Maoist Peoples' War ideology -- somehow involving every person in the armed struggle -- plays a large part in how the Chinese expect to conduct IO. Additionally, the notion that any means is acceptable given China's inferior position is gaining ground in at least some circles.[38] Finally, the ancient influence of Sun Tzu is often starkly evident, both explicitly and implicitly.[39] This includes incorporation of ideas about indirect approaches, asymmetry, and a balance between positive vs. negative, weakness vs. strength, force vs. guile. China often sees the laws of war, technology and balance of military power largely favoring the West, and they do not desire to be bound by that.[40] A major way to overcome this imbalance is through the use of stratagems, which will be covered later.

A Few Words on Terminology

Information and Information Systems

Before discussing many of the IO concepts found in the following chapters, the terms information and information systems must be defined. For our purposes, information is*content*: the raw or processed facts, data or ideas, no matter where they are stored or how they are

---

[37]Mao Tse Tung, "The Struggle in the Chingkang Mountains, November 25, 1928" reprinted in *Selected Writing of Mao Tse Tung*, (Ft. Leavenworth: Command and General Staff College Combat Studies Institute, undated), 94-97. This passage provides an excellent perspective on the Chinese Communistworld view of the time. This author's notes from Command and General Staff College Course A553, "China: Military Art, Wars and Revolution, and the People's Liberation Army" (Jan-Mar 2003) support the view of Chinese perceptions.

[38]Hawkins, Charles F. "The Four Futures: Competing Schools of Military Thought Inside the PLA," HERO Library, n.d. < http://www.herolibrary.org/THE%20FOUR%20FUTURES.htm> (September 17, 2002).

[39]Yoshihara, Toshi. *Chinese Information Warfare: A Phantom Menace Or Emerging Threat?* Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA: November 200, 26.

communicated. Information systems are in essence the *means* by which information is *handled*: hardware, people, organizations, medium, etc. See Appendix A for a further discussion on this topic.

Information Operations vs. Information Warfare

The U.S. Department of Defense has used the same working definition of IO for several years now. This makes comparison and contrast of doctrine a straightforward affair. Doctrine also differentiates between IO and information warfare (IW), with the latter being IO conducted in times of crisis or conflict.[41]

Writers outside of DOD, being unbound by our definitions, often still use the term "information warfare" to describe what the military calls IO. Some authors consider all incidences of high technology incorporated into military operations to be part of information warfare. This would include ISR sensors, digital C3 systems and precision munitions. Closely related to this view is the notion that all actions taken to achieve information superiority are part of information warfare. In other words, IM, ISR and IO are subsumed under the IW mantle.

The same issue often arises when reviewing Russian and Chinese definitions of IW, which are discussed in Appendix A. While this disagreement in terms can be confusing, careful study allows the reader to extract the concepts specifically related to IO as defined in U.S. doctrine. For clarity and consistency, this monograph will substitute the acronym IO for IW whenever the source is referring to what the U.S. defines as IO.

So far, this monograph has identified a problem in Army IO doctrine. It has also laid the groundwork for understanding the discussion that follows in terms of basic definitions and the context for using foreign ideas. It is now time launch into the heart of the argument: seeking the means to redress the problem.

---

[40]See Ming Zhang, "War Without Rules," in *Bulletin of the Atomic Scientists*. November/December 1999 (Vol. 55, No. 6), 16-18 <http:/www.bullatomsci.org/issues/1999/nd99zhang.html> September 8, 2002. This is a review of *Unresticted Warfare.*

CHAPTER THREE

DISCUSSION

> *New weapons of warfare call for the total and radical reorganization of methods of warfare, and he who falls asleep during this process of reorganization may never wake up.*
>
> *– M.N. Tukhachevskiy*[42]

This chapter consists of a review and analysis of appropriate literature from the U.S., Russia and China. At the end, there should be an appreciation for the concepts applicable to effectively combining the elements of IO, so that it is conducted in an integrated manner. This includes understanding the environment as well as analyzing specific ideas for their value in improving Army IO doctrine. This will include effects, systems, target models, and certain foreign concepts.

Environmental Factors Affecting the Conduct of IO

Back in the 19th Century, Clausewitz said war is about imposing your will on the enemy.[43] In the contemporary operating environment, military forces conduct more than just war. This monograph assumes that Clausewitz's dictum can be extrapolated to military operations other than war. No matter what the mission, commanders will seek to control their environment in order to accomplish their mission. In the 21st Century this includes the information environment. In seeking macro-level principles for combining IO elements, this environment has to be understood.

IO Crosses Multiple Domains

Army doctrine states that information activities within a commander's area of interest are likely to affect his or her operations. To understand these effects, commanders must consider the

---

[41]Department of Defense, *JP 1-02 DOD Dictionary of Military and Associated Terms* (2002) < http://www.dtic.mil/doctrine/jel/doddict/index.html> (February 10, 2003).

[42]Mikhael Tukhachevskiy, "New Problems in Warfare, 1931," Reprint of a U.S. Army War College reproduction of unpublished manuscript, 18-19, School of Advanced Military Studies, Fort Leavenworth, KS.

[43]Carl von Clausewitz, *On War*, eds. and trans. Michael Howard and Peter Paret, (Princeton, NJ: Princeton University Press, 1984), 75.

entirety of the information environment. The information environment includes the individuals, organizations and systems that collect, process or disseminate information; also included is the information itself.[44] According to MCWP 3-40.4, "IO targets information or information systems to affect the information-based decision-making process."[45] Through targeting information or information systems, IO ultimately seeks to influence human or machine-based decision processes.[46] These statements support the contention that directly or indirectly, IO practitioners dispute control of the information battlespace via three domains: physical, cognitive and information. The DOD Command and Control Research Program (CCRP) promulgates the following definitions for each domain[47]:

The physical domain is the place that people, weapons, and information systems (i.e., hardware) actually inhabit--on land, at sea, in air or space. It is the traditional sphere of military operations, where effects of fire and maneuver are generally identifiable and quantifiable.

The cognitive domain encompasses the human mind. It is where knowledge, "perceptions, awareness, understanding, beliefs and values reside," as well as the place where decisions are made.

Representations of the physical and cognitive domains are communicated through the information domain. These representations are created, manipulated and shared through this domain. This realm would include the electromagnetic spectrum and information in digitized form.

Edward Waltz is an engineer who has written an extensive textbook on information warfare. He agrees that the IO battlespace transcends the information realm, encompassing what he calls

---

[44]*FM 3-13*, 1-2.

[45]Department of the Navy. "MCWP 3-40.4 Information Operations (Coordinating Draft), December 10, 2001," Electronic copy of coordinating draft, p. 7, HQ, U.S. Marine Corps, Washington, D.C.

[46]JP 3-13, vii.

[47]David S. Alberts, John J. Gartska, Richard E. Hayes and David A. Signori, *Understanding Information Age Warfare*, revised ed. (Washington, D.C.: DOD C4ISR Cooperative Research Program, 2001), 12-14.

the physical and perceptual ones as well.[48] This concept has some significant implications, sometimes blurring the boundaries between IO and more traditional operations. The fact that IO takes place in three distinct domains represents a challenge in determining targets, desired effects, and assessment means.

IO Spans the Entire Depth of the Operational Environment

Since IO is conducted beyond just the physical domain, it offers the potential to expand what a commander can influence. Through IO, commanders can transcend boundaries of time and space that limit their traditional force capabilities. IO takes place during every phase of an operation.[49] Using IO, our adversary's reach exceeds those imposed by geographic constraints or political borders.[50] The converse is also true: we can affect adversaries and neutrals over extended time and distance. The Marines believe IO enhances their operations by influencing targets from a distance, thereby reducing their physical presence on scene.[51] Greater reach equates to greater depth of the battlespace, which brings both opportunities and challenges for IO soldiers.

Technology is an important factor in the multi-dimensional nature and extended depth of IO. The proliferation and improvement of technology have driven the rapid expansion of the information environment.[52] The ever-increasing openness and interdependence of networks, devices and data enables the rapid, efficient and often unlimited movement of information worldwide. Military command and control is increasingly dependent on this phenomenon. Therefore, IO can and does take advantage of the growingsophistication, connectivity and dependencies information technology brings to the modern operational environment.[53]

The expansion of information technology infrastructures helps link the globe in new ways. This link is central to the ability of IO elements to influence the military environment in all

---

[48]Edward Waltz, *Information Warfare: Principles and Operation.* (Boston: Artech House, 1998), 27.

[49]MCWP 3-40.4, 7.

[50]Ibid., 5.

[51]Ibid.

[52]*JP 3-13*, I-13 to I-14.

situations. National and global infrastructures allow voluminous and relatively inexpensive dissemination of information over extended distances. The proliferation of the Internet and handheld communications, along with radio and television, allow individuals, private groups, governments and mass media to spread their messages.[54] These factors provide the potential for friendly, neutral and adversary IO activities to reach new and expanded audiences, both intended and unintended. The ease of access offered by the information infrastructure also allows more friendly organizations to be involved in IO.

IO Involves a Wealth of Actors

It is not just military forces that are involved in IO. The global and technological foundations of IO create a situation where IO crosses over former boundaries between military, other governmental and even civilian realms. Effective IO requires the understanding, coordination, contributions and unity of numerous military and non-military activities that can affect the information environment. This is true for both the offensive and defensive sides of IO. Not just the Department of Defense (DOD), but a multitude of actors has interests, duties and ideas regarding IO. On the government side, there are other federal agencies, law enforcement organizations, and Congress. In the civilian sector, academia and information technology organizations, among others, have a stake.[55] IO practitioners should plan on using not just military capabilities, but interagency and multinational ones as well.[56]This phenomenon creates a tremendous scope of IO activity.

IO as an Integrating Strategy

The environmental factors discussed so far show the depth and scope of the IO environment. Taking advantage of opportunities while mitigating risk associated with this situation requires a huge effort on the part of all involved. That is why many IO proponents suggest IO is above all an

---

[53]Ibid., vii.
[54]*FM 3-0*, 1-14.
[55]*JP 3-13*, I-11, I-13.
[56]Ibid., V-1.

integrating strategy, albeit one that can affect combat power. As used here, strategy is defined as relating means to ends.[57]

The concept of IO has evolved from merely a vague notion of combining immature concepts and emerging methods to an integrating strategy.[58] As a strategy, IO integrates various capabilities and activities to achieve designated objectives, focused on the vulnerabilities and opportunities of adversary and friendly information and information systems.[59] It can assist planners and executors in identifying and coordinating the assets, tasks, targets and objectives of the operation.

The intent and concept statements are the commander's primary means for articulating how the unit will achieve its objectives. Ultimately, all operational activities must be unified towards this common purpose. This includes IO, whether the specific activity is offensive, defensive or influencing.[60]

Unity of effort always entails synchronization with higher and adjacent units.[61] For IO however, units must often leverage the assets and/or activities of non-organic entities to further their own IO objectives.[62] Information operations activities demand "early coordination between components, groups, organizations and agencies" engaged. Effective IO also entails de-confliction through constant coordination with higher, lower and parallel echelons as well as internally.[63] Coordination with other US entities and allies or coalition partners is often imperative.[64]

---

[57]Edward C. Mann II, Gary Endersby and Thomas R. Searle. *Thinking Effects: Effects-Based Methodology for Joint Operations* (Maxwell AFB, AL: Air University Press, 2002), 70.

[58]Andrew Garfield, "Information Operations as an Integrating Strategy: the Ongong Debate," in *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*, ed. Alan D. Campen and Douglas H. Dearth (Fairfax, VA: AFCEA International Press, 2000), 267.

[59]*JP 3-13*, I-3.

[60] MCWP 3-40.4, 6.

[61]Ibid.

[62]Ibid.

[63]*JP 3-13*, V-4 to V-5.

[64]Ibid., I-2.

Bringing together "various capabilities and activities to achieve designated objectives," as mentioned above, is an extremely difficult undertaking. It is time to get to the heart of how IO operates as an integrating strategy at a macro level. How to ensure the right targets are engaged in a manner that supports meeting the commander's objectives is largely an art. There is now, however, a more reliable mechanism that can assist commanders and staffs in this effort.

The Effects-Based Approach to IO

The effects-based operations (EBO) methodology provides a rigorous and rational mechanism for development of IO strategy. It logically explains the expected connections between IO actions, the expected outcomes caused by those actions, and how those expected outcomes support attainment of the commander's objectives.[65] It supports a systematic approach to conducting operations. It therefore has significant benefit for IO. There are many discussions on EBO available, including those by Air Force Brigadier General DavidDeptula and RAND Corporation's Paul Davis. This monograph primarily relies on the recent Air University Press paper by Edward Mann, Gary Endersby and Thomas Searle.

With EBO, actions taken against the enemy are designed to achieve specific effects that lead to the desired military and political objectives.[66] The Air Force believes using the effects-based approach to operations is fundamental to successful IO. This requires information operators to tie effects to objectives, then match the right mix of capabilities to get those effects.[67] This growing recognition that achieving desired effectssupercedes selection of targeting means should be inherent in our approach to IO.[68]

According to Mann, Endersby and Searle, effects "consist of a full range of outcomes, events, or consequences that result from a specific action." The effects-based approach is based upon

[65]Mann, et. al., 2.
[66]Ibid., 1.
[67]Department of the Air Force, *AFDD 2-5 Information Operations* (Washington, D.C.: GPO, 1998), 27-28.
[68]MCWP 3-40.4, 8.

planning for desired objectives with a focus on results, selecting targets to generate those desired results, and the expectation of execution causing secondary, tertiary and greater effects.[69] Figure 1 graphically demonstrates the concept.

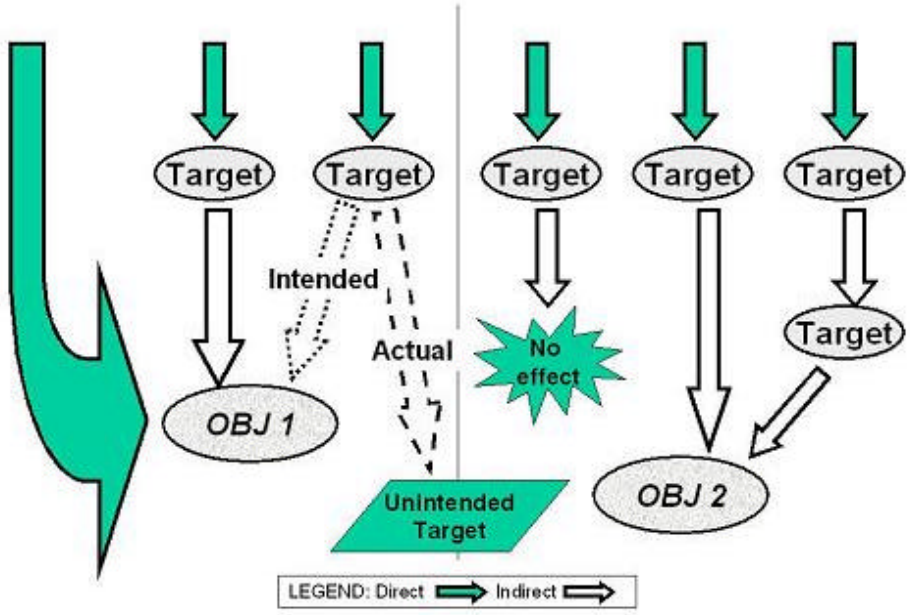

Figure 1. Graphic Example of Direct and Indirect Effects.

There are several different kinds of effects pertinent to this discussion. Commanders and staffs have to be concerned with these in order to understand how to apply EBO to IO. Table 1 lays out those definitions. What is important is that all these effects enter into the equation of IO achieving its desired outcomes in support of the commander's objectives.

Type of Effect	***Definition***
Direct (first order)	Immediate or nearly immediate outcomes of an action against a specific target and/or location[70]
Indirect (second order, third order and beyond)	Outcomes caused by and subsequent to an immediate (direct) or intermediate effect [71]
- Cumulative	An indirect effect resulting from an aggregate of direct and indirect effects that generally flow upward from a lower level of war[72]

[69]Mann, et. al., 30-31.
[70]Ibid., 32.
[71]Ibid.
[72]Ibid., 33.

- Cascading	An indirect effect resulting from an aggregate of direct and indirect effects that generally flow downward from a higher level of war[73]
Collateral (may be positive or negative)	An outcome, first order or otherwise, that was not intended by the causal action[74]
Physical	(Generally) direct effects of a physical nature caused by actions against an object or system[75]
Functional	Direct or indirect effects of action on the ability of a target to function properly/perform its mission[76]
Systemic	Indirect effects meant to affect the operation of a system or set of systems[77]

Table 1. Types of Effects.

An IO action may seek to achieve objectives through attaining the desired outcome through direct effects. However, if that is not possible, units can plan to take advantage of indirect effects of their actions. In this case, commanders and staffs plan cumulative or cascading effects to attain the ultimately desired outcome.[78]

A relatively simple scenario can exemplify the simultaneous use of all three types of effects. Consider how a friendly force might attempt to achieve its IO objective of deceiving an enemy corps commander as to the location of a friendly ground attack. The friendly force could allow a group of dummy tanks to be photographed by enemy satellites. A series of such photographs, once passed down from the enemy's national intelligence organization to the enemy commander, might create a cascading effect. If friendly forces jam the communications of the enemy's long-range reconnaissance teams, they cannot send reports up to the enemy commander. Not knowing they see the actual attack coming, he would be subject to cumulative effects created by the friendly jamming. Finally, by inserting false information on the enemy commander's computer via a computer network attack, friendly forces would create a direct effect on the enemy commander. All together, friendly actions created a series of direct and indirect effects that

[73]Ibid., 34.
[74]Ibid., 35.
[75]Ibid., 37.
[76]Ibid.
[77]Ibid., 38.
[78]Ibid., 31-34.

resulted in achieving the desired objective: deceiving the enemy commander about the location of the friendly attack.

There is usually the potential for collateral effects. Good IO plans seek to capitalize on desirable collateral effects, while minimizing the chances of undesirable ones.[79] Using an effects-based approach should ensure these possibilities are clearly understood by commanders and staffs as they conduct IO. This allows them to make logical choices throughout the military decision-making process. It is especially helpful during course of action development and analysis, and supports the risk assessment and mitigation decisions they go through.

Understanding the inherent linkages between physical, functional and systemic effects is important to planning, preparation, execution and assessment. It helps commanders and their staffs think through and articulate exactly what they need friendly actions to produce.[80]

Mann, Endersby and Searle propose a planning process for EBO. This process sheds further light on how EBO can assist in guiding commanders and staffs in conducting IO. The model has five parts: researching the environment; determining goals; developing a strategy; tasking and integration of elements to implement the strategy; and finally, assessing effects. Two of these planning activities, research and assessment, have particular relevance to development of macro-level guidance on combining IO elements. They raise important issues that commanders and staffs conducting IO at all levels should be aware of.

The Systems Approach

The research step in the EBO process is about gathering increasingly detailed information on adversaries, from the global level to the individual target. It covers what appropriate effects might be, and how they might be achieved and measured.[81] This represents a thorough sub-process based on an understanding of the effects likely to be caused up, down and across from the directly affected target. The research sub-process is firmly grounded in understanding the systems related

[79]Ibid., 35-36.
[80]Ibid., 38-39.

to the target.[82] A RAND Corporation study for the Air Force even includes the word systems in its definition of EBO: "operations conceived and planned in a systems framework that considers the full range of direct, indirect and cascading effects…"[83] So it seems that understanding systems is elemental to EBO.

A systems approach relates to effects-based thinking because it provides the understanding to identify where to act in order to create change in systems, which correlates to achieving effects. Insight and understanding gained from using a systems approach is imperfect. Still, it gives commanders and staffs a tool that better equips them to plan, prepare, execute and assess operations. They should be able to see how things are, how things work, how things relate, and how the command can affect the system to its advantage -- and change the future to look like the desired endstate.

The systems approach applies at two levels. The lower level is about understanding the inner workings of isolated systems. The upper level encompasses taking a holistic view of multiple, inter-related systems. Both are important to IO. The discussion below shows why a systems approach can be an important tool to guide commanders and staffs as they attempt to combine IO elements.

Webster's defines a system as "a regularly interacting or interdependent group of items forming a unified whole."[84] More specifically, this monograph is concerned with open systems, which better describe the living entities in the battlespace. Open systems receive inputs, transform the inputs in some way, and create outputs, all towards some purpose or aim.[85] In *The Logic of Failure*, psychology professor Dietrich Dorner describes another key part of a system, feedback.

---

[81]Ibid., 3.
[82]Ibid., 58-68.
[83]Paul K. Davis, *Effects Based Operations: A Grand Challenge for the Analytical Community*, (Santa Monica, CA: RAND Corporation, 2001), 7.
[84]"Merriam-Webster Online – The Language Cente,." Merriam-Webster, n.d. <http://www.webster.com/> (March 13, 2003).
[85]Shimon Naveh, "*In Pursuit of Military Excellence: The Evolution of Operational Theory*," (London: Frank Cass Publishers,1997), 5.

He defines a system as "a network of many variables in causal relationship to one another." He says understanding the existence of variables is important. However the way they affect themselves and others in the system, or feedback, gives insight into which variables to influence if you want to alter the system.[86] This is key because commanders, in wanting to act first, must shape their battlespace. This implies changing systems in their battlespace.

Understanding the way discrete systems in the battlespace work is important. The inputs, outputs, transformation process, feedback and aim of systems all offer the commander and staff ways to see strengths and weaknesses in those systems. Whether friendly ones which need to be protected, or adversary and other ones which may be leveraged, they represent possible points to apply combat power in trying to attain the commander's objectives.

Dorner cautions that reducing systems to their lowest level can be dangerous however, This overly simplistic, "reductionist" approach can lead to overconfidence. Another view, from the holistic side is required to fully appreciate the battlespace of a complete system. The commander and staff have to understand the feedback between discrete systems, and the affect it creates between and among systems in the battlespace.[87]

Management theorist Peter Senge makes the argument for "systems thinking." Senge believes systems thinking provides a way to see patterns that might otherwise be missed, and how to effectively change things.[88] It allows understanding inter-relationships and seeing the foundations of a complex environment, thereby presenting opportunities for leverage.[89] Systems thinking represents the higher level of the systems approach in this monograph.

In summary, a systems approach provides commanders and their staffs a cognitive way to see and understand the complex and unique combination of the terrain, physical objects, people, organizations and other things that is their battlespace. By seeing and understanding the

[86]Dietrich Dorner, *The Logic of Failure*, (New York: Metropolitan Books, 1996), 73-74.
[87]Ibid., 88-90.
[88]Peter M. Senge, *The Fifth Discipline: The Art & Practice of the Learning Organization* (New York: Currency-Doubleday, 1990), 7.

battlespace, they can better use an effects-based approach to plan, prepare, execute and assess operations that achieve decisive results. Determining how well commanders and staffs are moving towards achieving those decisive results requires constant and accurate assessment. The ability to assess, and gather information on systems inside the battlespace hinges upon another activity: intelligence, surveillance and reconnaissance (ISR).

The Importance and Challenges of ISR in Supporting IO

Both in the Army operations process and in the proposed EBO planning process, assessment is a constant activity. Assessment has to include determining all types of effects generated within the targeted systems, which is a difficult task.[90] Although the commander and his entire staff will be involved in assessing IO effects, they will rely heavily upon information and intelligence collected and produced by their ISR system.

Information operations, like other means to achieving military objectives, rely on ISR.[91] However, IO puts unusual and extremely specific demands on the intelligence community.[92] Concerned with more than just enemy order of battle factors, IO intelligence preparation of the battlefield (IO IPB) must analyze demographics, personalities, economics, culture and media in the area of operations.[93]

Helping measure the effects of IO against friendly, enemy and neutral elements will be a significant ISR challenge. Considering the means of attack, targets of attack, and desired effects, the results of offensive and defensive IO will often be less tangible than military leaders are used to. Given our current ISR capabilities are largely geared towards measuring effects on traditional, kinetic targets, good assessment becomes even more difficult. With human decision-making as its

---

[89]Ibid., 68-69.
[90]Mann, et. al., 75-76.
[91]*AFDD 2-5*, 21.
[92]JP 3-13, I-18.
[93]*FM 3-0*, 11-17.

ultimate target, commanders and their staffs will find it hard to ascertain whether IO actions are succeeding or failing.[94]

Early Army IO doctrine recognized the foundational role of intelligence in IO.[95] Over time, that recognition seems to have waned. As intelligence has morphed into ISR, IO and ISR have become equal contributors to information superiority. Nevertheless, the Army needs to follow the DOD lead and re-assert the special, critical relationship between ISR and IO.[96] In doing so, the commanders and staffs would more readily recognize the vitally important role of ISR in IO. In searching for macro-level guidance on combining the IO elements, this cannot be overlooked.

Pros and Cons of an Effects-based Approach

It is unnecessary for the Army IO community to immediately and completelydive into EBO. It is prudent, however, to borrow relevant aspects of EBO that can pay immediate dividends. The goal of the last several pages has been to articulate how IO can use effects to advantage. The perceived pluses and minuses are explained below.

Using an effects based approach potentially offers two major benefits for Army IO. First, it brings rigor to the process of relating means to ends, or strategy. This helps ensure that the right elements are matched to the right targets, to get the right effects, to attain the commander's objectives. The second benefit is its ability to provide insight into potential unintended effects that commanders and staffs need to constantly be aware of.

Looking at IO through an effects-based perspective also raises further ideas that possess potential application to IO. For one, it suggests good reasons for commanders and staffs to adopt

---

[94]Department of Defense, *Joint Vision 2020,* (Washington, D.C.: GPO, 2000), 29.

[95]Departent of the Army, *FM 100-6 Information Operations*, (Washington, DC, August 1996), Chapter 2 <http://155.217.58.58/cgi-bin/atdl.dll/fm/100-6/ch2.htm > (March 13, 2003).

[96]Department of Defense. "Department of Defense Directive 3600.1 Information Operations (Formal Coordination), n.d." Formal Coordination Draft obtained by the author via e-mail in Oct 02. Washington, D.C., Assistant Secretary of Defense (Command, Control, Communications and Intelligence), 2-3. This draft DOD policy makes Intelligence support to IO a fourth, distinctive activity, on the same level as core and supporting elements and related activities.

a systems approach to understanding the environment of IO. Additionally, it reminds commanders and staffs how important ISR is to their IO efforts.

An obvious shortcoming in the effects-based argument at present is the general way in which the word "effects" is thrown around. While the word is defined, the kinds of effects that commanders and staffs might want to achieve never are. This is one area that many, particularly in the Army, would like to see addressed. Fortunately, the need to look at non-lethal effects is noted by Mann, Endersby and Searle.[97]

The Army is moving forward by defining selected IO effects in FM 3-13.[98] Still, doctrine has a long way to go in helping commanders and staffs grasp this issue – promoting a common language is after all an area in which doctrine is supposed to excel.[99] This problem is big enough to rate its own document, so it will not be resolved here. However, Appendix B contains some useful information on the subject for future research, including some Russian thinking on the subject.

Another shortcoming is in EBO is the general way in which target selection is treated. Again, the term is used a lot, and references are made as to how EBO helps select targets. Yet there is no mention of a systematic means to do this. Such information could be of benefit to Army commanders and staffs.

IO Targets

According to JP 3-60, *Joint Doctrine for Targeting*, targets are areas, installations, forces, equipment, capabilities, functions or behaviors identified for possible action to support the commander.[100] Given this wide latitude of things that IO can engage to support the commander, how do he and his staff chose? Doctrine is generally vague on specific targets of IO. During the earlier discussion on domains, information, information systems, and human decision-makers

[97]Mann, et. al., 79.
[98]*FM 3-13*, 1-17 to 1-18.
[99]*FM 3-0*, 1-14.

were identified as potential IO targets. But you cannot drop leaflets or a precision guided munition on these largely intangible targets. So it appears again that some guidance is in order. Fortunately, there are several IO proponents who can provide such guidance.

The Russians appreciate the inherent complexities involved in conducting IO. They believe that the impact and actions of IO rely on modern, highly developed systems methodologies.[101] They are therefore increasingly modeling combat using a system-on-system approach rather than merely calculating overall ratios between the competing forces. Integration of these models, including looking at offensive and defensive IO, is also stressed.[102]

This sort of methodology might be useful to U.S. Army planners for use in IO targeting. Doctrinal models, or analogues, based on information systems, could be developed to help understand the battlespace, do predictive analysis, template facilities and activities, and develop plans.[103] Sources of potential analogues abound.

Georgetown University professor Dorothy Denning offers a functional breakout of what she calls "information resources," that might be considered as IO targets. First are containers, or any media that holds information. This includes human and computer memories, printed materials, and removable magnetic media such as tapes and disks. Second, are transporters such as couriers, vehicles, postal systems, point-to-point communications systems, radio, television and computer networks (from local area networks through the Internet). The third category, sensors, provides the means of extracting information from other objects or the environment. Cameras, microphones, scanners and the human senses fit this category. Recorders, which transfer information into containers, are the fourth category. Examples include printers and tape recorders.

---

[100]Department of Defense, *JP 3-60 Joint Doctrine for Targeting* (GPO: Washington, DC, January 17, 2002), GL-12.

[101]Vladimir Slipchenko, *Wars of the Sixth Generation* (Moscow: VECHE, 2002), references here are based on an informal translation of "Section 3.6: Information Counteraction in Wars of the Future" *(151-164)*, provided by Foreign Military Studies Office, Ft. Leavenworth, KS -- page references are to the hard copy provided, 4.

[102]Thomas, "Russian Understanding," 805-806.

[103]Gary Klein, *Sources of Power* (Cambridge, MA: MIT Press, 1998), 197.

The final category is information processors. These items, such as people and computers (including the hardware and software) are used to manipulate information. As the resources are interconnected to create a holistic information infrastructure, they also offer the possibility for IO to enter the system at one point while creating effects at another.[104] What Denning essentially provides is an information-based model of cyberworld targets. While geared to describing cyber activity, this model actually has broader value for planning, executing and assessing all types of IO activities. Figure 2 graphically portrays this model.

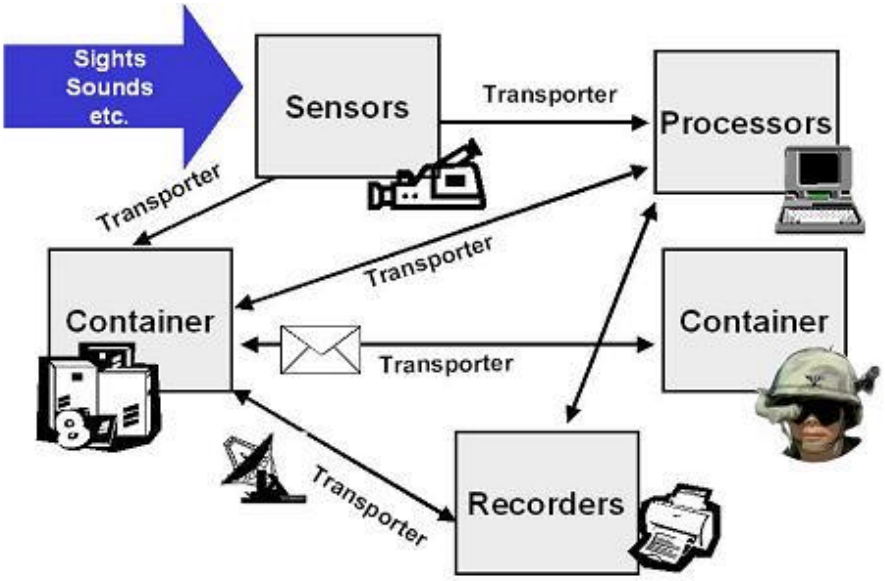

Figure 2. Information-based Targeting Model.

National Security Council staffer and U.S. Air Force officer GregoryRattray provides another model that can assist in IO targeting. Again focused on cyber activity, his book described four sets of components that comprise an information infrastructure: facilities and hardware, software and standards, information resources (media and data) and people. These components meld to support three types of activity: development and use of underlying technology; provision

[104]Dorothy E. Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999), 21-22.

of networks and services; and individual or organizational tasks.[105] This description allows framing a scalable model for targeting, this one based on domains. It presents users with three layers that IO can affect: the underlying technology layer; processing, storage and transmission layer; and human layer.[106] See Figure 3 for a graphic representation of this model.

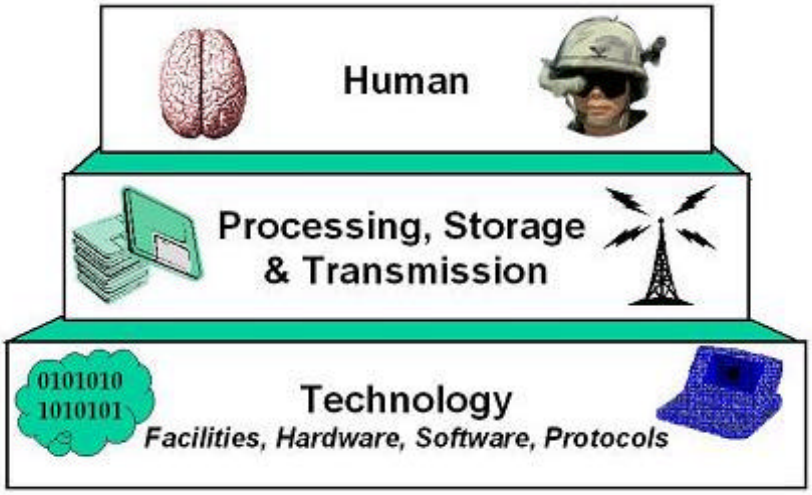

Figure 3. Domain-based Targeting Model.

Retired Russian Admiral Vladimir Pirumov and Russian Colonel M.A. Rodionov provide a different perspective on identifying IO targets. At the time they wrote their article, Pirumov, an EW expert, was Vice President of the Russian Academy of Natural Sciences, while Rodionov was a Candidate of Technical Sciences. Their concept combined an information-centric view with a military one. They described military information capabilities as derived from three related systems, or "components of information capability." The first is stored information, whether in written form, digital memory, audio-visual records (i.e. analog) or human memory. The second is information actually circulating within C3 systems, whether it is being collected, processed or transmitted. The third is C3 facilities and units themselves, including ISR organizations and assets, headquarters and command posts, communications units and assets, as well as navigation

[105]Gregory J. Rattray, Strategic Warfare in Cyberspace (Cambridge, MA: MIT Press, 2001), 32.

support systems (e.g. topographic, weather, hydrographic, etc.)[107] This description of military specific information systems provides a third discrete model for use in IO targeting.

Another Russian perspective on potential targets allows construction of yet another model; one based on military battlefield functions. It focuses on the "reconnaissance-strike and reconnaissance-weapon complexes," which are interconnected by the "infosphere–the programs that process, store and create data."[108] A reconnaissance-strike complex is essentially the C4ISR system, including personnel, automation and sensors. A reconnaissance-weapon complex refers to the information systems, personnel and arms actually on board weapon platforms.

The last ideas on the subject of target models come from the Chinese theorists.Major General Wang Pufeng, former head of the Academy of Military Sciences, offers what can be construed as model similar to the last Russian one. Wang says that IO is contended in the information detection, transmission, processing, usage and weapon-strike systems.[109] Dai Qingmin, a General Staff Departmental Director, offers a two-part model through his discussion on "information fighting means." He essentially notes how battlefield information will primarily flow via networked or electromagnetic means, or by electronic means, that is by radios through the electromagnetic spectrum.[110]

Figure 4 graphically portrays a hybrid model, combining all the Russian and Chinese ideas. It captures the idea that in military usage, information can be resident in a number of different places or forms. These places and things (recon, C3, weapons) and forms (stored, transmitted) can be said to represent the basic military functions and the links between them.

---

[106]Ibid, 33.

[107]Rear Adm. V.S. Pirumov and Col. M.A, Rodionov, "Information Warfare in Armed Conflict." *Military Thought (English Edition)* (Vol. 6, No. 5, 1997): 58.

[108]Thomas, "Russian Understanding," 801.

[109]Ma Yaxi, "Interview with Major General Wang Pufeng," *Hong Kong Hsien-Tai Chun-Shi (Conmilit)* in Chinese (April 11, 2000): 19-21. Translated and downloaded from the FBIS website. (February 11, 2003).

[110]Dai Qingmin, "Innovating and Developing View on Information Operations" *Beijing Zhongguo Junshi Kexue* in Chinese (August 20, 2000), 72-77. Translated and downloaded from the FBIS website (August 30, 2002).

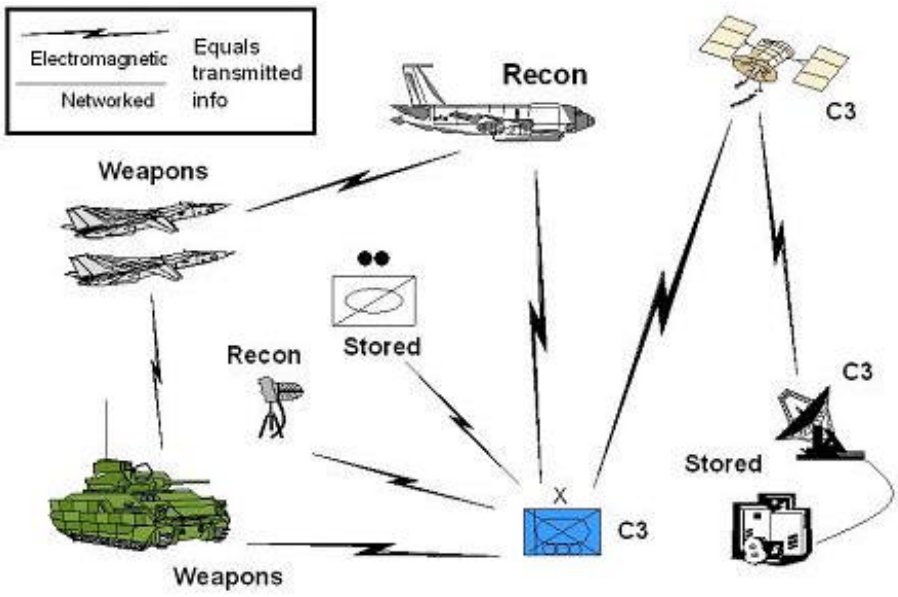

Figure 4. Military Function-based Targeting Model.

By applying the models above, commanders and their staffs can break their battlespace into constituent parts in order to identify where to target their IO effort. These conceptual, macro-level tools could be valuable time savers and support the effects-based approach to IO. They could help direct commanders and staffs in effectively combining IO elements towards the right targets to support achievement of unit objectives.

The Stratagem Approach to IO

An effects-based approach helps commanders and their staffs determine the most effective means to achieve their desired ends, or objectives. This approach is not the only method to determine ends, ways and means, however. The Chinese often rely on their historical traditions to determine the best approach to IO strategy by using the concept of stratagems for determining the best way to engage in an IO struggle.

The Chinese consider themselves materially and technologically inferior to many potential aggressors. To tip the balance in their favor, they stress outthinking their opponents. They see IO, like other types of warfare, as a strategic duel between commanders: outwitting the enemy's

decision-makers is the ultimate way to defeat them.[111] Historically and rationally, a focus on better strategy allows the Chinese IO practitioner to impose his will upon his adversary through superior thinking vice technology alone.[112] The traditional use of strategy is an easy and logical adaptation for the Chinese, reminiscent of the *36 Stratagems*, which may pre-date Christ.[113]

The work of several members of China's Command and Control Institute illustrates in some detail their modern application of stratagems fits into IO. The authors define IO stratagems as:

> "… schemes or methods devised and used by commanders and commanding bodies to seize and maintain information supremacy on the basis of using clever methods to prevail at a relatively small cost in information warfare."[114]

Within this context, the writers have given an exceptional amount of thought to the myriad of possible schemes and methods. They combine human and automated means to derive four main lines of IO stratagems.[115] Simply described, stratagems offer Chinese commanders and their staffs guidance on engaging enemy targets via multiple means and domains.

The first set of IO stratagems is based on "thinking contests." By influencing the enemy commander's knowledge and beliefs, these stratagems attempt to force enemy commanders into making poor decisions. The result is a situation that favors the Chinese. This type of stratagem can be achieved by using knowledge of the enemy commander's character and personality, or by merely developing superior plans, branches or sequels.[116] In thinking contests, the enemy is targeted through the cognitive domain.

The second set of IO stratagems is based on technology. With this type of stratagem, science and technology must be employed to achieve superiority over the enemy. This is done through employing better information systems than the enemy has, or using one's own systems to assist

---

[111]Yoshihara, 13.

[112]Dai Qingmin.

[113]"The Thirty-Six Strategies of Ancient China" <http://www.chinastrategies.com/intro.htm> August 30, 2002, 1.

[114]Niu Li, Li Jiangzou and Xu Dehui, "On Information Warfare Stratagems," *China Military Science* in Chinese (August 20, 2000), 115-122. Translated and downloaded from the FBIS website. (February 11, 2003).

[115]Ibid.

[116]Ibid.

the command in devising and executing superior plans.[117] This second set of stratagems targets the enemy through the information domain.

"Stratagems of a multi-dimensional contest" are the third set. This entails using assets in every spatial environment, such as land, sea, air or electromagnetic (EM), to gain information superiority. It also includes ensuring IO is integrated with other stratagems to achieve overall objectives, and using all the unit's intellectual assets to develop an optimal stratagem.[118] This set of stratagems actually uses all three domains – physical, cognitive and information – to target the enemy.

The last set of stratagems seeks to control the entire information process over time. This includes stratagems that ensure the integrity of the friendly information process, while disrupting the enemy system's integrity. These stratagems can also focus on attacking and protecting information systems at critical times.[119] This set of stratagems again uses all three domains, but Chinese writings seem to lean towards a heavy reliance on the information domain.

In essence stratagems help the commander and staff decide how to properly balance use of all three domains in acting on targets, especially the cognitive and information domains. The U.S. does not share the Chinese historic or cultural basis for using stratagems. Therefore, they do not offer a good alternative to EBO. However, the concept does have merit in coaching the commander and his staff how to think about the problem at hand. Remembering the four categories of stratagems may remind commanders and their staffs to find greater synergy in leveraging the cognitive and information domains.[120]

Chinese stratagems raise one more issue that EBO may not address very well. The last two sets specifically concern themselves with coordinating actions in time and space. This is a very important concern, considering the fact that proper integration of IO seeks to mass effects at the

[117]Ibid.
[118]Ibid.
[119]Ibid.
[120]Dai Qingmin.

decisive point faster than the adversary can. It is time and space that in fact define the decisive point. While EBO helps determine desired effects, there seems to be a need for another form of macro-level guidance to help commanders and staffs effectively combine IO elements in time and space. So the question is how do commanders and staffs determine what effects to mass where? That is the subject of the next major part of this discussion.

Arranging the IO Elements in Time, Space and Purpose

One Russian IO proponent, Col. M.A. Rodionov, produced a way for theorists to think about IO activity within a more traditional operational framework. He listed what he called forms of IO, which he described in the following manner. Information warfare operations are the combination of information battles, which are the combination of information actions, which are the combination of information strikes.[121]

Information strikes are defined as short, powerful and coordinated events targeting key adversary C2 systems, using EW, combined EW and fires (missiles, artillery and aviation included), computer software strikes, or special strikes (psychological attacks against personnel). The first two types are coordinated by time, depth and tasks. The latter two are coordinated by task, place and time.[122]

Col. S.A. Komov's views are related, but more detailed. He used the term information impact to describe a single application of means towards accomplishing a discrete IO task. Information attacks then, comprise a combination of impacts that address a discrete tactical task. The sum of impacts and attacks combined to create operational effects is labeled an information battle. Finally, an information operation is a specifically designed combination of impacts, attacks and battles that achieve theater or strategic objectives.[123]

---

[121]Col. M.A. Rodionov, "Forms of Information Warfare," *Military Thought (English Edition)* (Vol. 7, No. 2, 1998): 84-85.

[122]Ibid., 87-88.

[123]Col. S.A. Komov, "Forms and Methods of Information Warfare," *Military Thought (English Edition)* (Vol. 6, No. 4, 1997): 25.

Understanding these ideas may provide a useful framework for arranging IO activities. It may help U.S. Army commanders and staffs think through how to achieve effects in space and time so that they support an information operation or campaign. Slightly modifying the terms and ideas expressed by Rodionov and Komov, the following table presents a model for structuring U.S. Army IO activities and relating them to effects. Table 2 relates the structure to currently understood tasks and planning concepts for further clarity.

Term	***Place in hierarchy***	***Type of effect:***	***Fulfills:***	***Examples***
IO action	Effect of one action	Direct (1st order)	One air tasking order mission; one artillery fire mission; one deception task	1 x leaflet mission; 1 x CNA; 1 x jamming mission vs. fire direction nets; 1 x dummy assembly area
IO strike	Sum of actions over time & space	Indirect (2nd…nth order)	IO support at a decisive point	leaflet drops, jamming & deception against enemy forces defending a river crossing
IO engagement	Sum of strikes and individual actions over time and space	Indirect (2nd…nth order)	An element's task *or* commander's IO objectives	All PSYOP actions taken to complete task of degrading enemy 1st echelon morale; all PSYOP, PA, CMO and maneuver tasks completed in order to influence civilians to "stay put"
IO battle	Sum of engagements over time and space	Indirect (3rd … nth order)	Commander's IO concept	All three commander's IO objectives met: deceive enemy commander as to location of decisive operation, influence civilians to stay home & disrupt enemy air defense network

Table 2. IO Activities and Effects.

Summary

This chapter has reviewed and analyzed the environmental factors as well as a number of U.S., Russian and Chinese concepts that relate to the actual conduct of IO. The analysis offers some appreciation for the concepts applicable to effectively combining the elements of IO. The next chapter will use this appreciation, synthesizing the key ideas that will be the source of principles for suggesting a solution to the problem of Army IO doctrine.

CHAPTER FOUR

CONCLUSIONS AND RECOMMENDATIONS

The principles of war are heuristic devices: rules of thumb that offer a quick entry into the solution of a problem.

– Dr. James Schneider[124]

This monograph began with an assertion that doctrine lacks general, macro-level guidance on how to combine IO elements. Given this problem, the intervening pages described what U.S., Russian and Chinese writings say on the subject. This chapter will synthesize this information to draw a series of conclusions relevant to offering a solution to the problem. As the conclusions are presented, they will also be assessed for their relevancy. Once the assessment is complete, the conclusions will be presented as recommend principles to correct what doctrine appears to lack.

Determining Assessment Criteria

History, doctrine and theory often form the grounds for assessment criteria in monographs of this type. This monograph chooses to rely on doctrine, since there is no single benchmark for theory and a new concept like IO has no long or broad (or unclassified) history to draw upon.

It has been repeatedly mentioned that commanders and staffs plan, prepare, execute and assess IO. All operations follow this cycle of activities, which is known as the operations process. The operations process is driven by battle command.[125] Battle command involves visualizing the operation, describing it to subordinates, and directing their actions.[126]

"Visualize" includes assessing the factors of mission, enemy, terrain and weather, troops and support available, time and civil considerations (METT-TC). It also includes determining the elements of operational design, such as center of gravity, decisive points and lines of operation.[127] "Describe" includes development of an operational framework, relating operations in space and

[124]Robert R. Leonhard, *The Principles of War for the Information Age*, with an introduction by Dr. James J. Schneider (Novato, CA: Presidio Press, 1998), viii.

[125]*FM 3-0*, 6-1.

[126]Ibid., 5-1.

time, stating what the force must do and conditions of success.[128] "Direct" includes determining the actual synchronization of means to accomplish the mission.[129]

Battle command is the application of the leadership element of combat power.[130] Visualizing, describing and directing are therefore critical and consistent activities of commanders and their staffs. It is reasonable to conclude that any guidance that helps them conduct these activities is beneficial. Therefore, in terms of IO, any guidance on combining IO elements should support commanders and staffs as they attempt to visualize, describe and direct IO.

The Utility of Foreign IO

Before concluding, it seems useful to review what value the foreign IO theories brought to this discussion. The most important concept coming from Russia was their scientific approach, which provided more precise terminology and rigorous operational thinking than can generally be found in U.S. writings. On the Chinese side, their focus on overcoming superior technology through intellectual discipline and creativity is a good reminder for our Army. Their approach heavily influenced the realization that Army doctrine needs to acknowledge and leverage the three domains of IO. These two different styles, arising from fundamental cultural, philosophical and historical differences, as attitudes towards the West, were enlightening and worthwhile.

Conclusions

This portion of the monograph identifies which concepts in Chapter 3 are considered most salient to the development of macro-level guidance and why. It does so by assessing each concept in relation to the criteria above, so as to determine if they merit inclusion in the recommendations.

Domains

This monograph has shown that the IO battlespace encompasses the physical, cognitive and information domains. The physical domain is where battles are traditionally considered to take

---

[127]Ibid., 5-3 to 5-13.
[128]Ibid., 5-13 to 5-15.
[129]Ibid., 5-15.

place, largely because the effects are obvious. The IO elements offer ways to extend battle into the other domains. For example, PSYOP seek to affect the cognitive activities of enemy or neutral persons. Another example is computer network attack, which offers the potential to affect the capacity and functions of adversary information systems. The Chinese already show a depth of understanding of domains potentially surpassing those of the U.S. Through the use of stratagems, they are striving to combine activity in the cognitive and information domains to seek advantage over their adversaries. Information and information systems and their constituent parts span more than just tangible locations. Commanders and staffs therefore, must know the domain(s) in which each element can most effectively and/or efficiently operate. If they do not recognize that IO crosses domains, they cannot fully use the resources associated with the IO elements. This leads to the first conclusion of this monograph: *Commanders and staffs must understand and leverage all three domains of IO—physical, cognitive and information--help guide commanders and staffs on how in combining the IO elements.*

Understanding the three domains helps commanders and staffs *visualize* IO by assisting them in picturing the terrain in more than just a physical sense. In terms of *describing*, it gives commanders and staffs insights on ways to link the force to its objectives when physical references to the enemy seem irrelevant (logical lines of operations).[131]

Systems

Information operations involve multiple domains, a multitude of actors and technology enabling rapid and voluminous information flow. Commanders and staffs need a way to understand the complexities of this situation. A systems approach offers an excellent way of doing so. The value of systems is simple. Commanders and staffs break the environment down into constituent systems: military, political, social, economic, cultural, information, legal, etc.

---

[130]Ibid., 5-1.

[131]See FM 3-0, 5-8 to 5-9. See glossary for DOD definition. Army doctrine recognizes that during some types of operations, physical lines of operations will be very unclear or absent all together. Therefore

They analyze the individual systems as discrete entities. Then they look at how the systems interact with each other. This provides a synthesized, holistic picture of the environment. Through this process, they should be able to determine where to affect the system to create environmental changes favorable to mission accomplishment. This concept has immense value for IO, leading to the second conclusion of this monograph*: Commanders and staffs must identify, understand and leverage IO-related systems in the battlespace in order to effectively combine IO elements.*

Using systems helps *visualization* in several ways. This includes giving commanders and staffs a holistic appreciation of the enemy, troops available and civil consideration. It also assists in determining enemy and friendly sources of power or centers of gravity.

Effects

Once commanders and staffs understand the situation through domain and system recognition, they need to apply their understanding to gain an advantage. This is the realm of IO as an integrating strategy: determining how to combine IO means available in order to achieve objectives. The EBO methodology provides a mechanism for rational development of such a strategy. It logically links the outcome of actions to an objective, while considering what other effects, positive and negative, may be created during the process.[132] Using the effects-based methodology during strategy development adds rigor to a decision-making process that previously had been based largely on intuition and/or history. Having seen great value in applying the EBO methodology to IO, this monograph makes a third conclusion: *Commanders and staffs must determine desired IO effects that support the commander's objectives in order to effectively combine IO elements.*

Defining and determining desired IO effects support *visualization* by commanders and their staffs through assisting in determination of decisive points. It supports *describing* by determining what specific action forces must take and clearly designating what conditions lead to mission

---

they developed the idea of logical lines to help the commander orient actions toward objectives in the absence of reference to an enemy or physical location.

success. It logically synchronizes the employment of the commander's means, thereby providing *direction*.

Targeting Models

The next concept directly connects the previous two. Using the systems approach in conjunction with an effects-based approach enhances the ability of commanders and staffs to develop an integrated IO strategy. But these activities can be made more efficient and effective if commanders and staffs can already visualize the possible information systems they may encounter. The targeting models described in Chapter 3 offer them such an advantage. Applying these models will give them a theoretical starting point to examine the real world, eventually finding specific targets for action by IO elements. For this reason, this monograph's fourth conclusion is: *Commanders and staffs must identify IO targets that support achieving the desired effects in order to effectively combine IO elements.*

Identifying targets that support commanders and their staffs in achieving the desired effects can assist commanders and their staffs in *visualizing* the battlespace. It does that by supporting the assessment of enemy, friendly and other information systems for targeting purposes. It supports *directing* by synchronizing fires, intelligence and other means necessary for engaging targets.

Time, Space and Purpose

Since IO takes place in three domains over potentially huge distances, arranging activities to achieve desired effects is uniquely challenging. So far, the concepts provided offer a partial framework for doing this. Commanders and staffs have to fully comprehend how the IO elements must be combined in time, space and purpose. Understanding causal linkages through EBO methodology helps determine purpose. Identifying targets helps with the spatial aspect. To further tie it together, Russian theories on the hierarchy of IO activities seem useful. These theories can

---

[132]Mann, et. al., 1.

be used to develop a model for logically arranging IO activities to enhance understanding (See Table 2). Combining this model with the causal linkage model derived from EBO provides a fairly comprehensive graphic appreciation for what it takes to mass the effects of IO (see Figure 5 below). This combined model supports understanding how the activities of IO elements have to be related over time, across distances and linked purposes to achieve mass at the ultimate objective. This model graphically portrays this monograph's fifth conclusion: *Commanders and staffs must arrange IO activities in time, space and purpose to mass effects in order to effectively combine IO elements.*

This conclusion supports *describing* by relating operations in time and space. It supports *direction* by affecting synchronization of the commander's means to accomplish the mission.

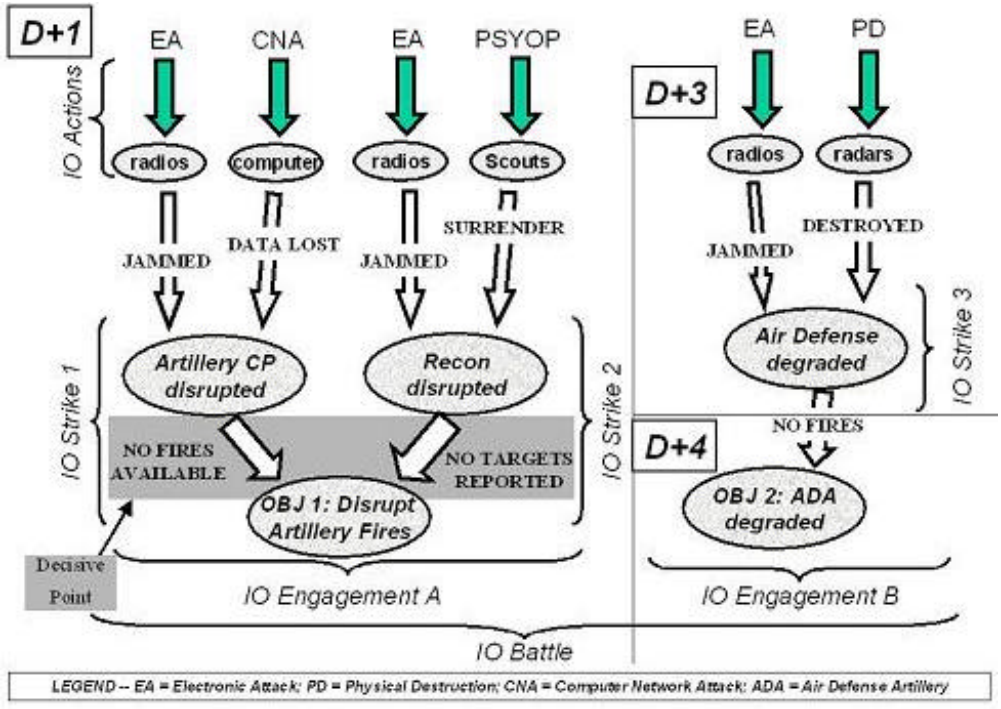

Figure 5. Arranging IO in Time, Space and Purpose.

ISR

Finally, the value of ISR in conducting IO cannot be overemphasized. Initially, ISR supports information gathering necessary to understand the three domains and the systems in the AO. This supports the research phase of EBO as well. As conduct of IO moves toward execution, ISR assists in defining what the optimum effects should be and where specifically to target IO activities to achieve those effects. During and after execution, the assessment of whether or not individual tasks and the operation as a whole have been accomplished will rely heavily on ISR contributions. Extremely detailed, timely and accurate intelligence is a prerequisite for successful IO. At all times, commanders and staffs have to ensure they focus ISR in time, space and purpose to get the answers they need for conducting IO. Therefore, this monograph asserts a final conclusion: *Commanders and staffs must direct and leverage ISR in order to effectively combine IO elements.*

Directing and leveraging ISR obviously supports *visualization* by providing the commander and staff a clear understanding of the enemy, terrain and civil considerations.

Chapter 1 included an assertion that FM 3-13 falls short in describing how to combine the IO elements at a macro-level. In reflecting upon the conclusions presented thus far, they may appear to form a logical sequence, a sort of process that provides a formula for how to combine IO elements. Yet some caution is in order.

In the following pages, the conclusions will become recommended principles for combining IO elements. The definition of "IO principles" used here is based on the doctrinal principles of war as described in FM 3-0. That FM never suggests that principles are sequential, or that they form a process. Further, some believe principles of war should be strictly adhered to. Conversely, another school of thought suggests that the principles of war should be seen as categories to assist military personnel with intellectually resolving the problems they face.[133] The intent of this monograph is not to create any rigid rules for commanders and their staffs. On the contrary, it is

meant to give them some broad intellectual boundaries that within whichis likely to lie the solutions to many of their challenges. A prescriptive process could have the unhealthy effect of leading commanders and staffs down paths that are either too narrow, or headed in the wrong direction. For that reason, the principles will stand alone.

That having been said, it is also clear that applying these principles can be a complex undertaking. Without guidance and expertise, commanders and staffs can wander aimlessly within the boundaries the principles create, never finding solutions they need. It would seem prudent that someone should be trained and educated to be the leader they need. Since IO is the topic, it seems reasonable to make the staff IO Coordinator that expert. It may be wise to ensure IO Coordinator is capable of doing so. Yet remembering the lessons learned in BCTP, it is unwise to absolve the commander and his staff from understanding these principles. They must all be responsible for knowing and applying the principles below as they integrate IO into full spectrum operations.

Recommendations

This monograph was based on the premise that U.S. Army doctrine does not provide general guidance for combining the IO elements, only a set of TTP. To redress this problem, the monograph reviewed U.S., Russian and Chinese IO doctrine and theories in a search for potential solutions. Upon analysis and synthesis of the literature, that search can be declared successful.

The outcome of that work is captured in the following recommendations for improving Army IO doctrine by including a set of principles to guide commanders and staffs in combining the IO elements. These principles are not presented in any prioritized or sequential order. They all provide generally valid and necessary guidance. The are presented in the form of a response to the question “What must commanders and their staffs do to combine the IO elements?” Each principle is followed with a short statement that expounds on the meaning and importance of the principle.

---

[133]Leonhard, 274-276.

- *Understand and leverage all three domains of IO: physical, cognitive and information.* Traditional military activities focus primarily on activities and effects in the physical domain. In attempting to affect and protect information, information systems, and decision-making processes, the activities and effects of IO take place in three domains. That is because facts, data and ideas (information) can be stored, processed and/or transmitted in physical objects (physical domain), the human mind (cognitive domain), digital or electromagnetic form (information domain) or combinations thereof. Commanders and staffs have to grasp the existence of and interconnections between these domains. Only then can they appreciate the opportunities and vulnerabilities inherent in the three domains, and their ability to leverage them to achieve their objectives.

- *Use a systems approach to understand the environment.* One of the best means of understanding the battlespace comes from considering it as a holistic system, with multiple subsystems. Commanders and their staffs analyze their battlespace from a systems perspective. They initially see the battlespace as one large system that is actually made up of many smaller systems. They consider the military, political, information, economic, cultural and other systems individually to understand each in sufficient detail to accomplish their mission. Then they investigate and identify the connections between systems and their interdependencies, so they understand the system from a holistic perspective.

- *Use an effects based approach.* IO is a strategy that integrates various capabilities and activities to achieve designated objectives, through affecting and protecting information and information systems. The effects-based approach supports strategy development by commanders and their staffs in two ways.

  - First, it provides them a rigorous method *for relating means to ends.* It helps determine effective linkages between IO actions, the effects they are expected to produce, and the attainment of the commander's objectives.

- Second, it is good *for recognizing the outcomes of actions, both desirable and undesirable*. By using an effects-based approach, commanders and staffs can logically develop and analyze courses of action and conceivably mitigate risk.

Effective use of the effects-based approach requires a clear understanding of the desired effects the commander and staff expect. This implies careful attention to the selection and definition of terms to describe the desired effect.

- *Use analogues to develop targets.* In conjunction with an effects-based approach, commanders and their staffs select targets. As they develop their IO integration strategy, commanders and staffs have to select the right targets to achieve effects they desire. Targeting models based on information systems provide an analogue for this purpose. Applying the models to the actual battlespace allows the commanders and their staffs to visualize what and where the potential targets are.

- *Arrange IO activities to mass effects.* Just like traditional operations, IO should be massed in time, space and purpose to mass on the decisive point. However, IO can be conducted over a more extended depth of time and space. The IO elements need not and often do act at the same physical location or same time as other elements of combat power. So it is useful to direct and control IO activities by arranging them through IO actions, engagements, strikes and battles each focused on achieving certain effects that ultimately serve a unified purpose of attaining designated objectives.

- *Leverage ISR to support the IO process.* All operations require some level of ISR support, but IO has exceptional demands. The timeliness, specificity and accuracy required to support IO is unique. Further, ISR is expected to collect and analyze information that can be extremely difficult to access, such as computer data or enemy or other leaders' opinions. Nevertheless, ISR must be tasked to provide critical input, especially during both strategy formulation and effects assessment, as commanders and staffs try to determine attainment of objectives.

Final thoughts

This monograph asserted that Army IO doctrine does not provide general, macro-level guidance on how to combine the IO elements. To alleviate this problem, the monograph recommended a set principles that could guide commanders and their staffs in combining the IO elements in order to meet commanders' objectives. This recommendation is based on analysis and synthesis of salient aspects of U.S., Russian and Chinese IO doctrine and theories.

The discussion of this topic should not end here. Certainly, arguments could be made for additional principles, and disagreement with the ones presented here is certainly possible. In fact, either would be welcome. This monograph merely furthers the debate on what IO doctrine should contain. There is a wealth of topics that arise from the discussion and recommendations in this monograph. Building a taxonomy for IO effects and developing an overarching American IO theory are just two tasks yet to be completed. The guiding principles for combining IO elements, as well as the other aspects of IO doctrine, are always subject to change. History, as well as new and improved theories will drive the evolution of doctrine, just as they always have. But for now, given the current body of theory and limited history of IO as a distinct concept, this monograph has presented a way to improve IO doctrine.

APPENDIX A

FURTHER DEFINING INFORMATION AND IO

Other Definitions of Information

DOD defines information as "1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation."[134] Arquilla and Ronfeldt describe two alternate views. They present the case for considering information as "message," encompassing everything within a pyramidal spectrum. Information starts as raw data, which through organization and processing can eventually become knowledge or even wisdom.[135] Waltz further by elaborates on the "message" concept by differentiating between the levels of stratum in terms of abstraction.[136]

Upon scrutiny, the DOD and "message" definitions are very close: they both key on content, considering facts/data as well as what the human mind does with them, to be information. Further, both definitions are unconcerned with the means of transmission. This leads to a common discussion as to whether or not the means of transmission is in fact information. Arquilla and Ronfeldt's second view is information as the "medium." This view incorporates not only the message, but also the mechanisms for communicating it between sender and receiver.[137] This second definition, is arguably more closely related to DOD's definition of information system, which is: "The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information."[138] Both of these definitions allude more to the instrumentality of communicating or handling the information.

For the purposes of this monograph, it was felt that the simple definitions provided in Chapter 2 would suffice. The more ethereal definitions presented above are merely presented to show the

---

[134]*JP 1-02.*

[135]John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp -- Section I" in *In Athena's Camp*, (Santa Monica, CA: RAND Corporation, 1997),145-146.

[136]Waltz, 51.

[137]Arquilla and Ronfeldt,146-148.

[138]*JP 1-02.*

complexity and diversity of thought on the issue, which may need further attention as Army IO doctrine continues to mature.

Russian Definitions of Information Operations

Like many American writers, Russians often use the term "information warfare." Yet it is clear that the Russian definitions of IW are very similar to U.S. definitions for IO. For example, most definitions are unambiguous in their statement that IW takes place in both peace and war--a statement true of US IO definitions. More importantly, most Russian writers state that IW is about two key things. First, "countermeasures," "influencing" or "suppression" of enemy information--in other words, attacking. Conversely, IW seeks to conduct "information defense measures" or "protect" friendly information, which correlates to US doctrine. Like some American theorists, Russians sometimes subsume the U.S. Army concept of information management under IW. They also tend to state the goal of IW is gaining information superiority.[139] While these amalgamations could lead to some confusion, a prior understanding allows fairly simple navigation through Russian IW writings. It is clear that the Russian term IW and U.S. term IO are so close that comparison and contrast are made relatively simple. Again, without an official doctrinal statement, Russian IO definitions must be regarded with caution.

Chinese Definitions of Information Operations

A distinct issue in assessing Chinese definitions of IW is their propensity to sometimes lump all things related to information into IW (like some U.S. authors do). For example, some authors consider combat using weapons or units that rely heavily on information technology, such as precision-guided munitions or the U.S. Army's digital division, as IW.[140] A good example of this propensity comes from a definition proposed by "Chinese experts" as quoted by WangBaucon and Li Fei of the Academy of Military Science, Beijing:

---

[139]Thomas, "Russian Understanding," 784-788.

[140]See Wang Baocun and Li Fei, "Information Warfare" in *Chinese Views of Future Warfare* (Revised Edition), Michael Pillsbury ed. Washington, DC: National Defense University Press, 1998, 328,

> "Information warfare is combat operations in a high-tech battlefield environment in which both sides use information-technology means, equipment, or systems in a rivalry over the power to obtain, control and use information. Information warfare is a combat aimed at the battlefield initiative; with digitized units as its essential combat force; the seizure, control, and use of information as its main substance; and all sorts of information weaponry [smart weapons] and systems as its major means…"[141]

For a number of other authors, IW is what warfare migrates to as information increasingly permeates conventional land, sea, air and space operations. Authors such as these see what the U.S. Army calls IO as a subset of their IW theory.

For the purposes of this monograph, ideas primarily associated with these broader IW theories were not considered. They are better described as "information-in-warfare."[142] For the others, pertinent ideas were extracted for discussion. One author succinctly says that the term "information warfare" equates to the American term "information operations."[143] The bulk of Chinese writings, however, demonstrate that this is an overly simplistic minority view. For the Chinese, warfare goes beyond Clausewitz's concept of the continuation of politics through violence.

Whether Russian and Chinese definitions sound similar to U.S. definitions, or in fact tend to lump terms together was not the point of this monograph. The point was how both countries envision integrating the means of IO through the use of certain principles, which differ from U.S. principles.

---

and Wang Pufeng, "The Challenge of Information Warfare," in *Chinese Views of Future Warfare*, 2d ed., ed. Michael Pillsbury, Washington, DC: National Defense University Press, 1998. 321.

[141]Wang Baocun and Li Fei, 328.

[142]"Information-in-warfare" is defined by the U.S. Air Force as "…extensive capabilities to provide global awareness throughout the range of military operations based on integrated intelligence, surveillance and reconnaissance (ISR) assets; … information collection/ dissemination activities; and … global navigation and positioning, weather, and communications capabilities. See in AFDD 2-5, 41.

[143]Sun Yujun, *Information Warfare: A Conceptual Understanding*, <http://www.herolibrary.org/p113.htm> September 4, 2002, 1.

APPENDIX B

TYPES OF IO EFFECTS

The value of IO is ultimately determined by "their effect on the enemy ability to execute military actions."[144] We did not state what some of those effects might be. Army commanders give subordinate units a task to accomplish, which in combination help the unit meet objectives and accomplish the mission. In a sense, IO activities can be given this same type of guidance through direction to achieve specific effects. In FM 3-13, the Army defines the following desired effects of offensive IO: destroy, degrade, disrupt, deny, deceive, exploit, and influence. No such specifics are given for defensive IO, but the words protect, defend, limit and counter appear in the one paragraph regarding the defensive function.[145] Informing non-adversaries and deterring unfavorable actions by enemies or other audiences are other uses of IO.[146]

The Joint Information Warfare Staff and Operations Course (JIWSOC) provides a rather exhaustive list of effects IO can achieve (see Figure 6), that can prove useful. What we are left with is providing specific meaning to these words, for many are not found in the DOD Dictionary. Even where they are found, they do not always readily translate to IO. We will not attempt to define them in the limited space here. The list alone will suffice for further analysis and synthesis. Yet they do offer a menu to guide commanders, IO planners and executors in determining what objectives IO should meet in support of the commander's concept.

[144]*FM 3-0*, 11-16.
[145]*FM 3-13*, 1-17 to 1-18.
[146]*MCWP 3-40.4*, 5-7.

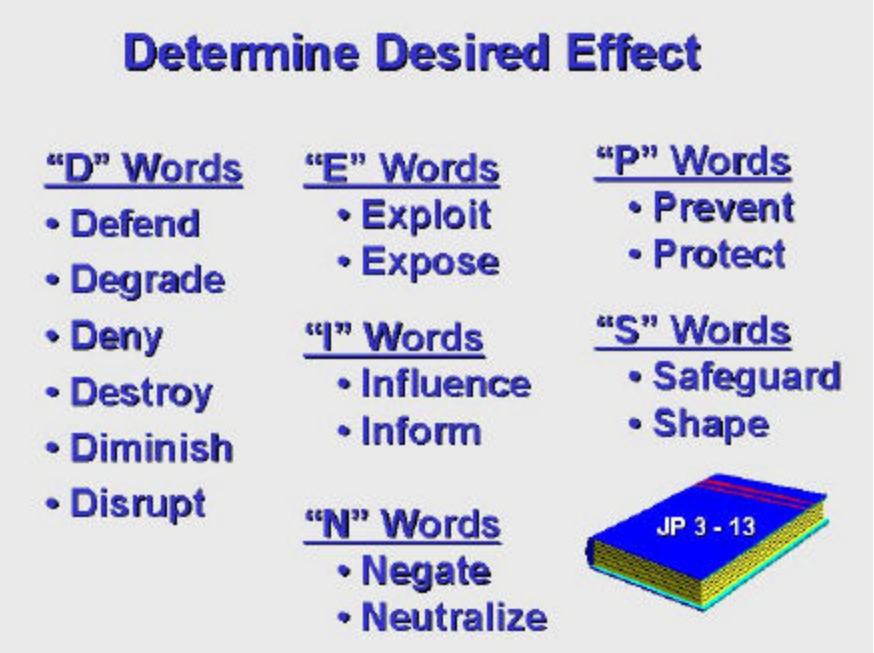

Figure 6. IO Effects List. Source: JIWSOC briefing, Class R-00-6, July 2000.

Some of words used to describe what Russian IO is expected to accomplish include "countermeasures," "disruption," "protection," "suppression," "defense" and "control." These terms probably seem understandable, reasonable and analogous to what U.S. audiences would call effects. However, another set of terms in Russian literature deals largely with more human aspects of IO--controlling the enemy.

These definitions were found amongst one Russian view of IO methods. Among those mentioned are blocking, detraction, exhaustion, appeasement, intimidation, provocation, overload, and pressure. Blocking is the process of complete or partial cessation of enemy's ability to collect or transmit information between nodes or platforms. Detraction is making the enemy believe in an actual or imagined threat to weak spots in their employment, and acting on that belief. Exhaustion is forcing the enemy to take unintelligent or wasteful actions, thereby reducing their physical and mental resources. Appeasement develops in the enemy the impression that friendly actions are not a threat, when in fact they are. Intimidation is making the enemy believe

that they are inferior to friendly forces, whether they are or not. Provocation is convincing the enemy to act in a manner that is actually advantageous to friendly forces. Overload is overwhelming the enemy's decision-making system with information, leading to reduced awareness on their side. Finally, pressure is feeding negative information about the enemy to various world audiences, with the goal of having public and institutional efforts interfere with enemy actions.[147]

[147]Komov, 23-25.

GLOSSARY

battlespace: the environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and information environment within the operational areas and areas of interest. (*FM 3-0*)

effects: a full range of outcomes, events, or consequences that result from a specific action. (*ACC EBO White Paper*)

effects-based: Action taken with the intent to produce a distinctive and desired effect. (*ACC EBO White Paper*)

effects-based operations: Actions taken against enemy systems designed to achieve specific effects that contribute directly to desired military and political outcomes. (*ACC EBO White Paper*)

full spectrum operations: the range of operations Army forces conduct in war and military operations other than war (*FM 3-0*)

lines of operation: Lines that define the directional orientation of the force in time and space in relation to the enemy. They connect the force with its base of operations and its objectives. (*JP 1-02*)

information: the raw or processed facts, data or ideas, no matter where they are stored or how they are communicated, that is content of a message (Author); Facts, data, or instruction in any medium or form. The meaning that a human assigns to data by means of the known conventions used in their representation. (*JP 3-13*)

information management: the provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decision making. It uses procedures and information systems to collect, process, store, display, and disseminate information. (*FM 3-0*)

information superiority: the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (*FM 3-0*).

information systems: Information systems are in essence the *means* by which information is *handled*: hardware, people, organizations, medium, etc. (Author); the equipment and facilities that collect, process, store, display and disseminate information. This includes computers—hardware and software—and communications, as well as policies and procedures for their use. (*FM 3-0*)

intelligence, surveillance and reconnaissance: An enabling operation that integrates and synchronizes all battlefield operating systems to collect relevant information to facilitate the commander's decision-making (*FM 3-0*)

objective : The clearly defined, decisive, and attainable goals towards which every military operation should be directed. 2. The specific target of the action taken (for example, a definite terrain feature, the seizure or holding of which is essential to the commander's plan, or, an enemy force or capability without regard to terrain features). (*JP 1-02*)

operation: 1. A military action or the carrying out of a strategic, operational, tactical, service, training, or administrative military mission. 2. The process of carrying oncombat, including movement, supply, attack, defense, and maneuvers needed to gain the objectives of any battle or campaign. (*JP 1-02*)

system: A regularly interacting or interdependent group of items forming a unified whole. (Webster's); A network of many variables in causal relationship to one another. (Dorner)

BIBLIOGRAPHY

Books

Alberts, David S., John J. Gartska, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. 2d revised ed. Washington, D.C.: DOD C4ISR Cooperative Research Program, 1999.

Alberts, David S., John J. Gartska, Richard E. Hayes and David A. Signori. *Understanding Information Age Warfare.* revised ed. Washington, D.C.: DOD C4ISR Cooperative Research Program, 2001.

Alberts, David S. *Information Age Transformation: Getting to a 21st Century Military*. Washington, D.C.: DOD Command and Control Research Program, 2002.

Arquila, Robert and Ronfeldt, David. *In Athena's Camp*. Santa Monica, CA: RAND, 1997.

Bunker, Robert J. *Information Operations and the Conduct of Land Warfare.* Arlington, VA: Institute of Land Warfare, Association of the United States Army, 1998.

Campen, Alan D. and Douglas H. Dearth, ed. *Cyberwar 2.0: Myth, Mysteries and Reality.* Fairfax, VA: AFCEA International Press, 1998.

Campen, Alan D. and Douglas H. Dearth, ed. *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict.* Fairfax, VA: AFCEA International Press, 2000.

Charlton, James, ed., *The Military Quotation Book*. New York: St. Martin's Press, 1990.

Clausewitz, Carl. *On War.* Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Davis, Paul K. *Effects Based Operations: A Grand Challenge for the Analytical Community.* Santa Monica, CA: RAND, 2001.

Denning, Dorothy E. *Information Warfare and Security.* Reading, MA: Addison-Wesley, 1999.

Deptula, David A. *Effects-Based Operations: Change in the Nature of Warfare*. Arlington, VA: Aerospace Education Foundation, 2001.

Dorner, Dietrich. *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations.* Translated by Rita and Rober Kimber. New York: Metropolitan Books, 1996.

Garfield, Andrew. "Information Operations as an Integrating Strategy: the Ongong Debate." In *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*, ed. Alan D. Campen and Douglas H. Dearth, 261-274. Fairfax, VA: AFCEA International Press, 2000.

Klein, Gary. *Sources of Power*. Cambridge, MA: MIT Press, 1998.

Leonhard, Robert R. *The Principles of War for the Information Age*. Novato, CA: Presidio Press, 1998.

Libicki, Martin C. *What is Information Warfare?* Washington, D.C.: National Defense University Press, 1995.

Mann, Edward C. II, Gary Endersby and Thomas R. Searle. *Thinking Effects: Effects-Based Methodology for Joint Operation*. Maxwell AFB, AL: Air University Press, 2002.

Mulvenon, James C. and Richard H. Yang. ed. *The People's Liberation Army in the Information Age*. Santa Monica, CA: RAND, 1999.

Naveh, Shimon. *In Pursuit of Military Excellence: The Evolution of Operational Theory*. London: Frank Cass Publishers, 1997.

Rattray, Greg. *Strategic Warfare in Cyberspace*. Cambridge, MA: The MIT Press, 2001.

Yoshihara, Toshi. *Chinese Information Warfare: A Phantom Menace Or Emerging Threat?* Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2001.

Senge, Peter M. *The Fifth Discipline: The Art & Practice of the Learning Organization*. New York: Currency-Doubleday, 1990.

Sun Tzu. *The Art of War*. Edited and translated by Samuel B.Griffith. London: Oxford University Press, 1971.

Waltz, Edward. *Information Warfare: Principles and Operations*. Boston: Artech House, 1998.

Wingfield, Thomas C. *The Law of Information Conflict: National Security Law in Cyberspace*, Falls Church, VA: Aegis Research Corporation, 2000.

Government Publications

Department of the Air Force. *AFDD 2-5 Information Operations*. Washington, D.C.: GPO, 1998.

Department of the Air Force. *ACC White Paper: Effects-Based Operations*. Langley Air Force Base, VA: Air Combat Command, 2002.

Department of the Army. *FM 3-0 Operations*. Washington, D.C.: GPO, 2001.

Department of the Army. *FM 3-01.11 Air Defense Artillery Reference Handbook*.Washington, D.C., 2000. <http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-01.11/toc.htm> (18 August 2002).

Department of the Army. *FM 3-13 Information Operations Doctrine, Tactics, Techniques and Procedures (Approved Final Draft)*. Washington, D.C.: GPO, 2002.

Department of the Army. *FM 3-90 Tactics*. Washington, D.C.: GPO, 2001.

Department of the Army. *FM 34-1 Intelligence and Electronic Warfare Operations*. Washington, D.C., 1994. <http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/34-1/CH1.HTM#1-3)> (18 August 2002).

Department of the Army. *FM 100-6 Information Operations*. Washington, D.C., 1996. <http://155.217.58.58/cgi-bin/atdl.dll/fm/100-6/ch2.htm> (March 13, 2003).

Department of the Army. *FM 34-1 Intelligence and Electronic Warfare Operations*. Washington, D.C., 1994. <http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/34-1/CH2.HTM#2-4> (18 August 2002).

Department of Defense. *Joint Vision 2020*. Washington, D.C.: GPO, 2000.

Department of Defense, *JP 1-02 DOD Dictionary of Military and Associated Terms* Washington, D.C., 2002. <http://www.dtic.mil/doctrine/jel/doddict/index.html> (February 10, 2003).

Department of Defense. *JP 2-0 Doctrine for Intelligence Support to Joint Operations.* Washington, D.C.: GPO, 2000.

Department of Defense. *JP 3-13 Joint Doctrine for Information Operations*. Washington, D.C.: GPO, 1998.

Department of Defense, *JP 3-60 Joint Doctrine for Targeting.* Washington, DC: GPO, 2002.

Land Information Warfare Activity. Fort Belvoir, VA: Land Information Warfare Activity, 1998.

Articles

Gauthier, Kathryn L. "China as a Peer Competitor? Trends in Nuclear Weapons, Space, and Information Warfare." In *The Dragon Awakes: China's Military Modernization Trends and Implications*, ed. Lawrence E. Grinter, 7-44. Maxwell Air Force Base, AL: U.S. Air Force Counterproliferation Center, 1999.

Thomas, Tim. *The Russian PSYOP and Information Operations Interface.* Ft. Leavenworth, KS: Foreign Military Studies Office, 1996.

Thomas, Tim. "Russian Views on Information-Based Warfare" In*Airpower Journal*, Special Edition 1996.

Thomas, Tim. "Human Network Attacks." *Military Review* (September-October 1999): <http://fmso.leavenworth.army.mil/fmsopubs/issues/humannet/humannet.htm> (August 30, 2002).

Thomas, Tim. "Chinese Electronic Strategies." *Military Review* (May-June 2001): <http://www.cgsc.army.mil/milrev/english/MayJun01/thomas.asp> (July 16, 2002).

Thomas, Timothy L. "The Russian Understanding of Information Operations and Information Warfare." In *Information Age Anthology: The Information Age Military.* ed. David S. Alberts and Daniel S. Rapp, 777-814. Washington, D.C.: DOD C4ISR Cooperative Research Program, 2001.

Thomas, Timothy L. "Russia's Asymmetrical Approach to Information Warfare." In*The Russian Military into the 21st Century*, ed, Stephen J. Cimbala. Frank Cass Publishers, 2001. A copy of this article was provided to the author by Mr. Thomas.

Triplett, William C. III. "Potential Applications of PLA Information Warfare Capabilities to Critical Infrastructures." In *People's Liberation Army After Next*, ed. Susan M. Puska, 79-106. Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2000.

Translated Documents

Chang Mengxiong. "Weapons of the 21st Century." In *Chinese Views of Future Warfare*, 2d ed., ed. Michael Pillsbury, 249-260. Washington, DC: National Defense University Press, 1998.

Dai Qingmin. "Innovating and Developing View on Information Operations." *Beijing Zhongguo Junshi Kexue* in Chinese. August 20, 2000, 72-77. Translated and downloaded from the Foreign Broadcast Information Service (FBIS) website. (August 30, 2002).

Guo Anhua and Zhang Haitian. "Increase Sense of Times, Vigorously Explore Laws." *Beijing Jiefangjun Bao* in Chinese. July 21, 1998, 6. Translated and downloaded from the FBIS website. (August 30, 2002).

Gao Yan. "Dangerous 'Unrestricted Warfare' – And What To Make of the Current International Order and Rules." *Hong Kong Ta Kung Pao* (Internet Version-WWW) in Chinese. March 13, 2000. Translated and downloaded from the FBIS website. (February 11, 2003).

Komov, Col. S.A. "Information Warfare in Modern War: Theoretical Problems." *Military Thought (English Edition)* (May-June 1996): 76-80.

Komov, Col. S.A. "Forms and Methods of Information Warfare." *Military Thought (English Edition)* (Vol. 6, No. 4, 1997): 22-26.

Kostin, Lt. Gen N.A. "Information Warfare Theory." *Military Thought (English Edition)* (Vol. 6, No. 3, 1997): 53-59.

Niu Li, Li Jiangzou and Xu Dehui. "On Information Warfare Stratagems." *China Military Science* in Chinese. August 20, 2000, 115-122. Translated and downloaded from the FBIS website. (February 11, 2003).

Ma Yaxi, "Interview with Major General Wang Pufeng." *Hong Kong Hsien-Tai Chun-Shi (Conmilit)* in Chinese. April 11, 2000, 19-21. Translated and downloaded from the FBIS website. (February 11, 2003).

Mao Tse Tung. "The Struggle in the Chingkang Mountains, November 25, 1928." Reprinted in *Selected Writing of Mao Tse Tung*. (Ft. Leavenworth, KS: Command and General Staff College, Combat Studies Institute, undated).

Pirumov, Rear Adm. V.S. and Col. M.A, Rodionov. "Information Warfare in Armed Conflict." *Military Thought (English Edition)* (Vol. 6, No. 5, 1997): 56-61.

Qiao Liang and Wang Xiangsui. *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House, 1999. Translated by Foreign Broadcast Information Service. Terrorism

Research Center, Inc. n.d. <http://www.terrorism.com/documents/unrestricted.pdf> (January 18, 2000).

Rodionov, Col. M.A. "Forms of Information Warfare." *Military Thought (English Edition)* (Vol. 7, No. 2, 1998): 84-88.

Slipchenko. Vladimir. *Wars of the Sixth Generation.* (Moscow: VECHE, 2002). Informal translation of "Section 3.6: Information Counteraction in Wars of the Future" (151-164) provided by Foreign Military Studies Office, Ft. Leavenworth, KS.

Tukhachevskiy, Mikhael. "New Problems in Warfare, 1931." Reprint of a U.S. Army War College reproduction of unpublished manuscript. School of Advanced Military Studies, Fort Leavenworth, KS.

Wang Baucon. "A Preliminary Analysis of Information Warfare." *Beijing Zhongguo Junshi Kexue (China Military Science)* in Chinese. November 20, 1997, 102-111, Translated and downloaded from the FBIS website. (February 11, 2003).

Wang Baucon and Li Fei. "Information Warfare." In *Chinese Views of Future Warfare,* 2d ed., ed. Michael Pillsbury, 327-341. Washington, DC: National Defense University Press, 1998.

Wang Pufeng. "The Challenge of Information Warfare." In *Chinese Views of Future Warfare,* 2d ed., ed. Michael Pillsbury, 317-326. Washington, DC: National Defense University Press, 1998.

Wei Jincheng "Information War: A New Form of People's War." In *Chinese Views of Future Warfare* (Revised Edition), ed. Michael Pillsbury, 409-412. Washington, DC: National Defense University Press, 1998.

Monographs, Reports, Theses, and Unpublished Works

Department of Defense. "Department of Defense Directive 3600.1 Information Operations (Formal Coordination), n.d." Formal Coordination Draft obtained by the author via e-mail in Oct 02. Washington, D.C., Assistant Secretary of Defense (Command, Control, Communications and Intelligence).

Farris, Kate. "Chinese Views on Information Warfare, 2000." Essay. Joint Maritime Operations, Naval War College, Newport, RI.

Department of the Navy. "MCWP 3-40.4 Information Operations (Coordinating Draft), December 10, 2001." Electronic copy of coordinating draft. HQ, U.S. Marine Corps, Washington, D.C.

Schneider, James J. "How War Works: The Origins, Nature and Purpose of Military Theory, 2001." Unpublished paper. School of Advanced Military Studies, Ft. Leavenworth, KS.

Tavenner, Carson. "Towards an Understanding of People's Liberation Army Information Warfare Doctrine." M.A. thesis, University of Washington, 2000.

Other Internet Sources

Coffman, LTC Donna L. "OPMS to OPMS XXI: Then, Now and the Future - What does it mean to the Quartermaster officer?" Quartermaster Professional Bulletin. Autumn 1997. <http://www.quartermaster.army.mil/oqmg/Professional_Bulletin/1997/Autumn/opmsxxi.html> (March, 13, 2003).

Hawkins, Charles F. "The Four Futures: Competing Schools of Military Thought Inside the PLA." HERO Library. n.d. <http://www.herolibrary.org/THE%20FOUR%20FUTURES.htm> (September 17, 2002).

Hollis, Roy. "Information Operations Observations, TTP, and Lessons Learned." Center for Army Lessons Learned. November 2001. <http://call.army.mil/products/trngqtr/tq3-02/hollis.htm> (March 3, 2003).

"Merriam-Webster Online – The Language Center." Merriam-Webster. n.d. <http://www.webster.com/> (March 13, 2003).

Ming Zhang, "War Without Rules." In *Bulletin of the Atomic Scientists*. November/December 1999 (Vol. 55, No. 6), 16-18. <http:/www.bullatomsci.org/issues/1999/nd99zhang.html> (September 8, 2002).

Nikitin, Alexander. "From REF to EAR: Russian Concepts of 'Seventh Generation' War." June 2001. <www.boell.de/downloads/medien/russianconcept.pdf> (September 22, 2002).

Sun Yujun, "Information Warfare: A Conceptual Understanding", HERO Library. February, 1999. <http://www.herolibrary.org/p113.htm> (September 4, 2002).

Szafranski, Richard. "A Theory of Information Warfare." Air University. 1995. <http://www.airpower.maxell.af.mil/airchronicles/apj/szfan.html> (September 4, 2002).

"The Thirty-Six Strategies of Ancient China." *n.d*. <http://www.chinastrategies.com/intro.htm> (August 30, 2002).

Thomas, Tim. "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operation (CALL Publication #98-21)". Center for Army Lessons Learned. 1998. <http://fmso.leavenworth.army.mil/fmsopubs/issues/dialect.htm> (August 30, 2002).

Thomas, Tim. "Like AddingWings to the Tiger: Chinese Information Warfare Theory and Practice." Foreign Military Studies Office. n.d. < http://call.army.mil/fmso/fmsopubs/issue/chinaiw.htm> (July 16, 2002).